

TWISTED GALOIS STRATIFICATION

IVAN TOMAŠIĆ

ABSTRACT. We prove a direct image theorem stating that the direct image of a Galois formula by a morphism of difference schemes is equivalent to a Galois formula over fields with powers of Frobenius. As a consequence, we obtain an *effective* quantifier elimination procedure and a precise algebraic-geometric description of definable sets over fields with Frobenii in terms of twisted Galois formulae associated with finite Galois covers of difference schemes.

CONTENTS

1. Introduction	1
2. Local study of difference schemes and their morphisms	4
2.1. Difference schemes vs. pro-algebraic varieties	4
2.2. Local Properties	8
2.3. Étale morphisms of difference schemes	11
2.4. Babbitt's decomposition	13
3. Bi-fibered structure of the category of difference schemes	17
4. Effective difference algebraic geometry	19
5. Galois stratification	21
5.1. Galois stratifications and Galois formulae	21
5.2. Direct Image Theorems	23
5.3. Quantifier elimination for Galois formulae	28
References	30

1. INTRODUCTION

Galois stratification, originally developed through work of Fried, Haran, Jarden and Sacerdote ([10], [7], [9]), provides an explicit arithmetic-geometric description of definable sets over finite fields in terms of Galois formulae associated to Galois coverings of algebraic varieties. When compared to the earlier work of Ax [2], made more explicit by Kiefe [14], which showed that every formula in the language of rings is equivalent to a formula with a single (bounded) existential quantifier, the fundamental achievement of the Galois stratification was the *effective* (in fact *primitive recursive*) nature of its quantifier elimination procedure. Moreover, the precise description of formulae in terms of Galois covers was particularly well-suited for applications of geometric and number-theoretic nature, for example in Fried's

Date: October 16, 2012.

2000 Mathematics Subject Classification. Primary 03C60, 11G25. Secondary 14G10, 14G15.

Key words and phrases. difference scheme, Galois stratification, Galois formula, Frobenius automorphism, ACFA.

work on Davenport's problem [8]. In our opinion, the most impressive application was in the work of Denef and Loeser on arithmetic motivic integration in [5]. They assign a Chow motive to a Galois formula, thus extending the consideration of algebraic-geometric invariants of algebraic varieties to arbitrary first-order formulae.

We develop the theory of *twisted Galois stratification* in order to describe first-order definable sets in the language of *difference rings* over algebraic closures of finite fields equipped with powers of the Frobenius automorphism. A (normal) *Galois stratification* on a difference scheme (X, σ) is a datum

$$\mathcal{A} = \langle X, Z_i/X_i, C_i \mid i \in I \rangle,$$

where $X_i, i \in I$ is a partition of X into finitely many normal locally closed difference subschemes of X , each $(Z_i, \Sigma_i) \rightarrow (X_i, \sigma)$ is a Galois covering with some group $(G_i, \tilde{\Sigma})$ and C_i is a conjugacy domain in Σ_i , with all these notions precisely defined in [19]. The *Galois formula* associated with \mathcal{A} is the realisation subfunctor $\tilde{\mathcal{A}}$ of X defined by the assignment

$$\tilde{\mathcal{A}}(F, \varphi) = \bigcup_{i \in I} \{x \in X_i(F, \varphi) : \varphi_x \subseteq C_i\} \subseteq X(F, \varphi),$$

where (F, φ) is an algebraically closed difference field and the conjugacy class $\varphi_x \subseteq \Sigma$ is the local φ -substitution at x , as defined in [19, Section 4]. Our principal result in its algebraic-geometric incarnation is the following *direct image theorem*, stating that a direct image of a Galois formula by a morphism of finite transformal type is equivalent to a Galois formula over fields with Frobenii. Equivalently, the class of Galois formulae over fields with Frobenii is closed under taking direct images by morphisms of finite transformal type (a precise statement is 5.13).

Theorem 1.1. *Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of finite transformal type (over a suitable base), and let \mathcal{A} be a Galois stratification on X . We can effectively compute a Galois stratification \mathcal{B} on Y such that for all (suitable) $(\bar{\mathbb{F}}_p, \varphi)$ with a high enough power of Frobenius φ ,*

$$f(\tilde{\mathcal{A}}(\bar{\mathbb{F}}_p, \varphi)) = \tilde{\mathcal{B}}(\bar{\mathbb{F}}_p, \varphi).$$

A model-theoretic restatement of the above theorem is that fields with Frobenii allow *quantifier elimination* in the language of Galois formulae. In other words, any definable set over fields with powers of Frobenius can be described by a Galois formula (a precise statement is 5.16).

Theorem 1.2. *Let $\theta(x_1, \dots, x_n)$ be a first-order formula in the language of difference rings (with suitable parameters). We can effectively compute a Galois stratification \mathcal{A} of the difference affine n -space such that for all (suitable) $(\bar{\mathbb{F}}_p, \varphi)$ with a high enough power of Frobenius φ ,*

$$\theta(\bar{\mathbb{F}}_p, \varphi) = \tilde{\mathcal{A}}(\bar{\mathbb{F}}_p, \varphi).$$

Conversely, every Galois formula is equivalent to a first-order formula in the language of difference rings over fields with Frobenii.

Historically speaking, the comparison of our result to the known model-theoretic quantifier elimination result found by Macintyre [16] and greatly refined in modern terms by Chatzidakis and Hrushovski [4], is parallel to the relation between the work of Fried-Sacerdote and the work of Ax mentioned above. Macintyre and Chatzidakis-Hrushovski show that any formula $\theta(x_1, \dots, x_n)$ in the language of

difference rings is equivalent, modulo the theory ACFA of existentially closed difference fields, to a Boolean combination of formulae of the form

$$\exists y \psi(y; x_1, \dots, x_n),$$

where ψ is quantifier free, and $\psi(y; x_1, \dots, x_n)$ implies that y satisfies a nonzero polynomial whose coefficients are σ -polynomials in x_1, \dots, x_n , i.e., the single existential quantifier is bounded. Their proof uses the compactness theorem and, although recursive, their quantifier elimination is far from being primitive recursive or effective in a suitable sense of the word.

The main achievement of our paper is the *effectivity* of our quantifier elimination procedure, the proof of the direct image theorem being fundamentally algorithmic and algebraic-geometric in nature. We show that our quantifier elimination and the decision procedure for fields with Frobenii are \dagger -*primitive recursive*, i.e., primitive-recursive reducible to basic operations in difference algebraic geometry, as detailed in Section 4. Although primitive-recursive algorithms are not known at the moment for some of the most elementary constructions in difference algebra, we strongly believe that in the near future our procedures will be shown to be primitive recursive. Needless to say, while it may be possible to start with the model-theoretic quantifier elimination and deduce the precise form of 1.2 (in fact 5.18), taking this route would be missing the point.

The statement 1.2 is over fields with Frobenii and that is why we must refer to the present author's Chebotarev Lemma [19, 5.30] which uses the difficult paper [13] on twisted Lang-Weil estimates, proving the earlier conjecture of [16] that ACFA is the elementary theory of fields with Frobenii. This is the only use of the main result of [13] in this paper, and the remaining references to [13] are mostly foundational lemmas. However, our Galois stratification procedure works over existentially closed difference fields unconditionally, *without* the use of [13], see 5.18.

One of the biggest challenges was the correct formulation of the result and even a suitable definition of a *Galois cover*, which already requires the full power of the theory of *generalised difference schemes* developed in [19], since the category of *strict* difference schemes has no reasonable Galois actions, coverings or quotients. One clear advantage of the description of the definable sets in terms of (twisted) Galois stratifications is our ability to reduce considerations regarding points on definable sets to calculations of various character sums, as expounded in [19]. Since the style of our proof is reminiscent of many a direct image theorem from algebraic geometry, our results should appeal to algebraic geometers and number theorists and we expect more diophantine applications to follow.

Our approach to the proof of 1.1 (in fact of 5.13) is more geometric and conceptual than those of [10], [7], [9] in the classical case. The proof from [17] in the algebraic case uses the theory of the étale fundamental group in a rather sophisticated way, which is not available in the difference scenario. However, by performing a ‘baby’ Stein factorisation at the start of our procedure, the only remnant of that theory is the short exact sequence for the étale fundamental group, in which case we can ‘manually’ keep track of what happens at the level of finite Galois covers. From this point of view, even if we were to eliminate all the difference language, our line of proof would still yield an essentially new proof in the classical case. Here, on the other hand, we must treat several genuinely new difference phenomena which do not arise in the algebraic case. Key ingredients include Babbitt's decomposition theorem 2.42 and our Chebotarev lemma [19, 5.30].

Although the foundation of the theory of generalised difference schemes has been laid in [19], for the purposes of this paper we must develop the framework even further in Section 3.

In the course of the proof, we use local properties of difference schemes previously unknown in difference algebraic geometry, developed in Section 2. It must be emphasised that our theory is almost orthogonal to the various notions of smoothness that appear in G. Giabiconi's thesis, see 2.26.

En route to the main theorem, we encounter another merit of working in the context of generalised difference schemes, a difference version of Chevalley's theorem 5.8, which gives a sufficient condition for the image of a morphism of difference schemes of finite transformal type to contain a dense open set. Wibmer gives a similar result by generalising difference algebra in a slightly different direction [20].

The author would like to thank Michael Fried, Angus Macintyre and Thomas Scanlon for fruitful discussions on the topic of this paper, and to Zoe Chatzidakis for pointing out the importance of Babbitt's decomposition to him many years ago.

2. LOCAL STUDY OF DIFFERENCE SCHEMES AND THEIR MORPHISMS

The foundation of the theory of generalised difference schemes started has been laid in [19]. The familiarity with this work is crucial and we freely use the concepts defined there, although the reader acquainted with [13] can follow the subsequent developments that refer to ordinary difference schemes.

2.1. Difference schemes vs. pro-algebraic varieties. One of the most important ideas in the study of difference algebraic geometry was the realisation that there is a translation mechanism between the language of difference schemes and that of algebraic correspondences, or, more generally, systems of prolongations associated with a difference scheme.

We would like to be able to reduce the study of certain local properties of difference schemes to the study of known properties of algebraic schemes through systems of prolongations. In order to achieve this goal, we must be able to speak about *difference subvarieties* of ordinary algebraic varieties, which is achieved by defining a *difference scheme associated to a scheme*.

Proposition 2.1 ([13]). *Let (R, σ) be a difference ring. The forgetful functor from the category of difference (R, σ) -schemes to the category of locally R -ringed spaces has a right adjoint $[\sigma]_R$, i.e., for every R -scheme X we have a morphism $[\sigma]_R X \rightarrow X$ inducing the functorial isomorphism*

$$\mathrm{Hom}_R(Z, X) = \mathrm{Hom}_{(R, \sigma)}(Z, [\sigma]_R X),$$

for every (R, σ) -difference scheme (Z, σ) , where the morphisms on the left are the morphisms of locally R -ringed spaces.

Suppose now that X is an R -scheme and (Z, σ) is a closed (R, σ) -difference subscheme of $[\sigma]_R X$. For ease of notation, let us write $S = \mathrm{Spec}(R)$. Writing X^{σ^n} for $X \times_S S$ where the morphism $S \rightarrow S$ is σ^n , it is clear that the σ^n -linear morphism $\sigma^n : [\sigma]_R X \rightarrow [\sigma]_R X$ defines an R -morphism $[\sigma]_R X \rightarrow X^{\sigma^n}$ and thus we deduce a morphism

$$Z \hookrightarrow [\sigma]_R X \rightarrow X \times X^{\sigma} \times \cdots \times X^{\sigma^n} =: X[n].$$

We denote the scheme-theoretic image of this map by $Z[n]$, obtaining a closed R -subscheme $Z[n] \hookrightarrow X[n]$ for every n . Although the projective limit $Z[\infty]$ of the

$Z[n]$ can be viewed as a scheme, we will find it most illuminating to view it as a pro-(scheme of finite type).

The maps $X^{\sigma^{n+1}} \rightarrow X^{\sigma^n}$ induce the maps $\sigma : X[n+1] \rightarrow X[n]$ and thus $X[\infty]$ is equipped with an endomorphism induced by σ . In particular, this defines an isomorphism $\sigma : \prod_{n \geq 1} X^{\sigma^n} \rightarrow \prod_{n \geq 0} X^{\sigma^n} = X[\infty]$. We also have the projection $r : \prod_{n \geq 0} X^{\sigma^n} \rightarrow \prod_{n \geq 1} X^{\sigma^n}$.

Proposition 2.2 ([13]). *An R -subscheme Y of $X[\infty]$ is of the form $Z[\infty]$ for some difference subscheme (Z, σ) of $[\sigma]_R X$ if and only if Y contains rY^σ .*

We say that Z is *weakly Zariski dense* in X if $Z[0] = X$. Note that it can happen that Z is weakly Zariski dense in X but the set of points of Z is not Zariski dense in X .

Let us now start with a difference scheme (X, σ) of finite σ -type over (R, σ) and build a system of ‘prolongations’ of X in which X is weakly Zariski dense by construction. We shall describe the procedure for an affine difference scheme $(X, \sigma) = \text{Spec}^\sigma(A)$, where $A = R[a]_\sigma$ is an (R, σ) -algebra of finite σ -type, generated by a tuple $a \in A$.

If we write $A_n := R[a, \sigma a, \dots, \sigma^n a]$, we have inclusions $A_n \hookrightarrow A_{n+1}$ and maps $\sigma_n : A_n \rightarrow A_{n+1}$ induced by σ , so that (A, σ) is the direct limit of the A_n and the σ_n . We obtain the following diagram for $X_n = \text{Spec}(A_n)$.

$$\begin{array}{ccccccc}
 S & \longleftarrow & X_0 & \longleftarrow & X_1 & \longleftarrow & X_2 \longleftarrow \dots \\
 \uparrow \sigma & & \uparrow & \nearrow \sigma_0 & \uparrow & \nearrow \sigma_1 & \uparrow \nearrow \sigma_2 \\
 S & \longleftarrow & X_0^\sigma & \longleftarrow & X_1^\sigma & \longleftarrow & X_2^\sigma \longleftarrow \dots \\
 & & \nwarrow & & \nwarrow & & \nwarrow \\
 & & X_0 & \longleftarrow & X_1 & \longleftarrow & X_2 \longleftarrow X_3 \longleftarrow \dots
 \end{array}$$

By construction, we have closed immersions $X_1 \hookrightarrow X_0 \times_S X_0^\sigma$ and $X_{n+1} \hookrightarrow X_n \times_{X_{n-1}^\sigma} X_n^\sigma$ for $n \geq 1$, and we conclude that we have written (X, σ) as a weakly Zariski dense difference subscheme of X_0 .

Lemma 2.3 (Preparation Lemma). *With above notation, if A and R are algebraically integral and all $A_n \rightarrow A_{n+1}$ are separable, by σ -localising A and R we can arrange that morphisms*

$$X_{n+1} \rightarrow X_n \times_{X_{n-1}^\sigma} X_n^\sigma \rightarrow X_n \times_{X_{n-1}} X_n$$

are isomorphisms for $n \geq 1$ and that X is a Zariski dense difference subscheme of X_0 .

Proof. Let K be the fraction field of R . By combining the statements 5.2.10, 5.2.11, 5.2.12 from [15], modulo a σ -localisation of R , we can find a new tuple of generators $a = bc$ so that, writing $\sigma^i(a) = a_i = b_i c_i$ and $L_n = K(a_0, \dots, a_n)$ for the fraction field of A_n , we have that for $n \geq 1$,

- (1) b_n is algebraically independent over L_{n-1} , and
- (2) $[L_n : L_{n-1}(b_n)] = [L_{n+1} : L_n(b_{n+1})]$.

Given a diagram

$$\begin{array}{ccc} k & \longrightarrow & B \\ \sigma \downarrow & & \downarrow \sigma \\ C & \longrightarrow & K \end{array}$$

of sub- k -algebras B, C of a difference field (K, σ) , we shall say that B is σ -linearly disjoint from C over k if whenever $\{\beta_1, \dots, \beta_r\} \subseteq B$ is linearly independent over k , then $\{\sigma(\beta_1), \dots, \sigma(\beta_r)\}$ is linearly independent over C . This is equivalent to the injectivity of the natural map $B \otimes_k C \rightarrow \sigma(B)C$.

Using (1), we see that $L_{n-1}(b_n)$ is σ -linearly disjoint from L_n over L_{n-1} , and using (2) we deduce that L_n is σ -linearly disjoint from $L_n(b_{n+1})$ over $L_{n-1}(b_n)$. By transitivity of σ -linear disjointness, it follows from the diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & L_{n-1} & \longrightarrow & L_{n-1}(b_n) & \longrightarrow & L_n \longrightarrow \cdots \\ & & & \searrow \sigma & \searrow \sigma & \searrow \sigma & \\ & & & & L_n & \longrightarrow & L_n(b_{n+1}) \longrightarrow L_{n+1} \longrightarrow \cdots \end{array}$$

that L_n is σ -linearly disjoint from L_n over L_{n-1} for all $n \geq 1$.

Now, using generic freeness [11, Lemme 6.9.2], by σ -localising A (by an element of A_0) we may assume that $\pi_{10} : A_0 \rightarrow A_1$ and $\sigma_0 : A_0 \rightarrow A_1$ are free (i.e., A_1 is a free A_0 -module both via π_{10} and σ_0), so $A_1 \otimes_{A_0} A_1$ is a free A_0 module. Thus the natural morphism

$$(A_1 \otimes_{A_0} A_1) \rightarrow L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1)$$

is injective, the kernel in general being the A_0 -torsion of $A_1 \otimes_{A_0} A_1$, which we thoughtfully made trivial. Moreover, by linear disjointness guaranteed by the construction,

$$\begin{aligned} L_0 \otimes_{A_0} (A_1 \otimes_{A_0} A_1) &= (L_0 \otimes_{A_0} A_1) \otimes_{L_0} (L_0 \otimes_{A_0} A_1) \\ &= L_0[A_1] \otimes_{L_0} L_0[A_1] \rightarrow L_0[A_1, \sigma(A_1)] = L_0[A_2] \end{aligned}$$

is injective. We conclude that $A_1 \otimes_{A_0} A_1 \rightarrow A_2$ is injective and thus bijective by the construction, and that both $\pi_{21} : A_1 \rightarrow A_2$ and $\sigma_1 : A_1 \rightarrow A_2$ are free. This is all we need to proceed by induction and prove that all

$$A_n \otimes_{A_{n-1}} A_n \rightarrow A_n \otimes_{A_{n-1}^\sigma} A_n^\sigma \rightarrow A_{n+1}$$

are isomorphisms. Note, if we are happy to finish with the associated morphisms being just closed immersions which are generically isomorphisms, we can skip the ‘generic freeness’ step and we do not need to localise A but only R . \square

Definition 2.4. Let P be a property of scheme morphisms of finite type. Consider the following permanence properties of P :

- (1) (Composite). A composite of morphisms with property P has property P .
- (2) (Base change). If $X \rightarrow Y$ has P , and $Z \rightarrow Y$ is arbitrary, then $X \times_Y Z \rightarrow Z$ has P .
- (3) (Open embedding). If $X \rightarrow Y$ has P , and $U \hookrightarrow X$, then $U \rightarrow Y$ has P .
- (4) (Genericity in the target). If $f : X \rightarrow Y$ (with Y integral) is generically P , there is a localisation Y' of Y such that $f \upharpoonright f^{-1}(Y')$ is P .

- (4') (Genericity in the source). If $f : X \rightarrow Y$ (with Y integral) is generically P , there is a localisation X' of X and Y' of Y such that $f \upharpoonright X' \cap f^{-1}(Y')$ is P .

We say that P is *hereditary* if it has properties (1)–(3). It is *hereditarily generic in the target (resp. source)*, if it is hereditary with property (4) (resp. (4')). The property P is *strongly hereditary* if in addition,

- (5) (SH). If $g \circ f$ and g have P , then f has P .

Definition 2.5. (1) Let (X, σ) be an (R, σ) -difference scheme of finite σ -type.

We say that (X, σ) has the property σ - P , if there exists a prolongation sequence X_n as above for X such that all the structure maps $X_n \rightarrow \text{Spec}(R)$ have the property P .

- (2) Let P be a property of scheme morphisms of finite type. Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of finite σ -type. We say that f has the property σ - P , if for every open affine $V = \text{Spec}^\sigma(R)$ in Y , the scheme $f^{-1}(V)$ has the property σ - P .

- (3) Let P be a property of morphisms of schemes of finite type. Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of schemes of finite σ -type (over some common base). We say that f has the property σ - P , if there exists a prolongation sequence $f_n : X_n \rightarrow Y_n$ for f such that all the maps f_n have the property P .

Remark 2.6. Suppose P is strongly hereditary.

- (1) If (X, σ) is σ - P , then all the connecting morphisms $X_{n+1} \rightarrow X_n$ have the property P .
- (2) If a morphism $f : (X, \sigma) \rightarrow (Y, \sigma)$ of schemes of finite σ -type (over some common base) is σ - P , and (Y, σ) is σ - P , then (X, σ) is σ - P .

Proposition 2.7. (1) Let P be a property of scheme morphisms of finite type which is hereditarily generic in the source/target. Then the property σ - P is σ -generic in the source. In other words, if $f : (X, \sigma) \rightarrow (Y, \sigma)$ is a morphism of finite σ -type which is generically σ - P , then there exists a σ -localisation X' of X and Y' of Y such that $f \upharpoonright X'$ is σ - P above Y' , i.e., $f \upharpoonright X' \cap f^{-1}(Y')$ is σ - P .

- (2) The same statements apply when P is a (target/source) hereditarily generic property of morphisms of schemes of finite type and $f : (X, \sigma) \rightarrow (Y, \sigma)$ is a morphism of schemes of finite σ -type.

Proof. Let us prove (2), the proof of (1) being strictly easier. We shall assume the reader has constructed, upon a σ -localisation of the source, the relevant diagram of prolongations for $f_n : X_n \rightarrow Y_n$ using the Preparation Lemma 2.3. In the case of genericity in the target, by using (G), modulo a σ -localisation of Y we can assume that $X_0 \rightarrow Y_0$ has P . Using (G) and (O), by σ -localising X by an element of X_0 we can assume that $X_1 \rightarrow X_0$ also has P .

In the case of genericity in the source, using (G), by a σ -localisation of X and Y we can assume that $X_0 \rightarrow Y_0$ has P . Using (G) again, we need to σ -localise X further to make $X_1 \rightarrow X_0$ have the property P . Using (O), the new $X_0 \rightarrow Y_0$ still has P , but we lose the exact σ -generation in terms of fibre products to the extent that $X_{n+1} \rightarrow X_n \times_{X_{n-1}}^\sigma X_n^\sigma$ are no longer isomorphisms for $n \geq 1$, but only open immersions.

We proceed by induction. Assuming that $X_{n-1} \rightarrow Y_{n-1}$ and $X_n \rightarrow X_{n-1}$ have P , using (C), we get that $X_n \rightarrow Y_n$ has P . Moreover, using (BC), we obtain that

$X_n \times_{X_{n-1}} X_n \rightarrow X_n$ has P . By (O) and the fact that $X_{n+1} \hookrightarrow X_n \times_{X_{n-1}} X_n$ for $n \geq 1$, we can deduce that $X_{n+1} \rightarrow X_n$ also has P , which keeps the induction going.

Let us note that, in case of a property strongly hereditarily generic in the target, if the preparation lemma could be improved so that we need only localise the base, then we could prove that σ - P is σ -generic in the target. \square

Corollary 2.8. *Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of finite σ -type.*

- (1) *If f is separable then there is a σ -localisation X' of X and Y' of Y such that $f \upharpoonright X' \cap f^{-1}(Y')$ is σ -smooth.*
- (2) *If f is separable algebraic, then there is a σ -localisation X' of X and Y' of Y such that $f \upharpoonright X' \cap f^{-1}(Y')$ is σ -étale.*

Corollary 2.9. *Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of finite σ -type whose generic fibre is geometrically integral. Then there is a σ -localisation Y' of Y such that $f \upharpoonright f^{-1}(Y')$ has geometrically integral fibres.*

Proof. If f has generic fibre which is geometrically integral, then without loss of generality f has generically σ -geometrically integral fibres. By the proposition, there is a σ -localisation X' of X and Y' of Y such that $f \upharpoonright X'$ has σ -geometrically integral fibres above Y' , so in particular f has geometrically integral fibres above Y' . \square

Corollary 2.10. *Let (X, σ) be an (R, σ) -difference scheme of finite σ -type which is separable. There is a σ -localisation X' of X and R' of R such that X'/R' is normal (in the sense of 2.22).*

Proof. By 2.8, take a σ -localisation X'/R' which is σ -smooth. \square

2.2. Local Properties. This subsection is mostly concerned with the question of whether it is reasonable to expect that if a property holds locally, at every point of a fixed point spectrum of a difference ring, then it also holds globally.

Definition 2.11. Let (M, σ) be an (A, σ) -module and let (N, σ) be a submodule.

- (1) We say that (M, σ) is *well-mixed* if $am = 0$ implies $\sigma(a)m = 0$ for all $a \in A$, $m \in M$.
- (2) We say that (N, σ) is a *well-mixed submodule* of (M, σ) if the module M/N is well-mixed.

Clearly (M, σ) is well-mixed if and only if the annihilator $\text{Ann}(m)$ of any $m \in M$ is a well-mixed σ -ideal in (A, σ) . Indeed, if $ab \in \text{Ann}(m)$, then $a(bm) = 0$ so $\sigma(a)(bm) = (\sigma(a)b)m = 0$ and $\sigma(a)b \in \text{Ann}(m)$.

Moreover, since the intersection of well-mixed submodules is well-mixed and M is trivially a well-mixed submodule of itself, for every submodule (N, σ) of (M, σ) there exists a smallest well-mixed submodule $[N]_w$ containing N . Thus $[0]_w$ is the smallest well-mixed submodule of (M, σ) associated with the largest well-mixed quotient M_w of M .

Proposition 2.12. *Let (M, σ) be a well-mixed (A, σ) -module. The following are equivalent.*

- (1) $M = 0$;
- (2) $M_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$.
- (3) $M_{\mathfrak{p}} = 0$ for every \mathfrak{p} maximal in $\text{Spec}^\sigma(A)$.

Proof. It is clear that (1) implies (2) and (2) implies (3). Suppose that (3) holds but $M \neq 0$. Let $x \in M \setminus \{0\}$ and let $\mathfrak{a} = \text{Ann}(x)$. Then $\mathfrak{a} \neq (1)$ is well-mixed and, by [19, 3.23], $V^\sigma(\mathfrak{a}) \neq \emptyset$. Choose a maximal \mathfrak{p} in $V^\sigma(\mathfrak{a})$. Since $x/1 = 0$ in $M_{\mathfrak{p}}$, there exists an $a \notin \mathfrak{p}$ such that $ax = 0$, which is in contradiction with $\text{Ann}(x) \subseteq \mathfrak{p}$. \square

Corollary 2.13. *Let (M, σ) be an (A, σ) -module. If $M_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$, then $M_w = 0$.*

The above can be sharpened as follows.

Proposition 2.14. *Let (M, σ) be an (A, σ) -module. If $(M_{\mathfrak{p}})_w = 0$ for every \mathfrak{p} maximal in $\text{Spec}^\sigma(A)$, then $M_w = 0$.*

Proof. Using the universal properties of localisation and passing to well-mixed quotients, as well as the fact that localisation is an exact functor, we construct a commutative diagram

$$\begin{array}{ccccc}
 M & \xrightarrow{\psi} & M_{\mathfrak{p}} & & \\
 \pi \downarrow & & \downarrow \pi' & \searrow \pi_{\mathfrak{p}} & \\
 M_w & \xrightarrow{\alpha} & (M_{\mathfrak{p}})_w & \xrightarrow{\beta} & (M_w)_{\mathfrak{p}} \\
 & \searrow \psi' & & & \uparrow \\
 & & & & (M_w)_{\mathfrak{p}}
 \end{array}$$

in which π and π' are surjective, so we conclude that $\pi_{\mathfrak{p}}$ and β are also surjective. Therefore, $(M_{\mathfrak{p}})_w = 0$ implies that $(M_w)_{\mathfrak{p}} = 0$ and we finish by 2.12. \square

Proposition 2.15. *Let $\phi : (M, \sigma) \rightarrow (N, \sigma)$ be an (A, σ) -module homomorphism and assume that (M, σ) is well-mixed. The following are equivalent.*

- (1) ϕ is injective;
- (2) $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is injective for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$.
- (3) $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is injective for every \mathfrak{p} maximal in $\text{Spec}^\sigma(A)$.

Proof. (1) \Rightarrow (2). If $0 \rightarrow M \rightarrow N$ is exact, since localisation is exact, we get that $0 \rightarrow M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is also exact. (2) \Rightarrow (3) is trivial.

(3) \Rightarrow (1). Let $M' = \ker \phi$. Then $0 \rightarrow M' \rightarrow M \rightarrow N$ is exact so $0 \rightarrow M'_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is exact for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$. By assumption, $M'_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$. Since M' is well-mixed (as a submodule of M), by 2.12 we conclude that $M' = 0$. \square

Proposition 2.16. *Let $\phi : (M, \sigma) \rightarrow (N, \sigma)$ be an (A, σ) -module homomorphism. If $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is almost surjective for every \mathfrak{p} maximal in $\text{Spec}^\sigma(A)$, then ϕ is almost surjective, $[\text{im}(\phi)]_w = N$ (equivalently, $\text{coker}(\phi)_w = 0$).*

Proof. Let $N' = \text{coker}(\phi)$. Then $M \rightarrow N \rightarrow N' \rightarrow 0$ is exact, and by localisation $M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}} \rightarrow N'_{\mathfrak{p}} \rightarrow 0$ is exact for every $\mathfrak{p} \in \text{Spec}^\sigma(A)$. By assumption, $(N'_{\mathfrak{p}})_w = 0$ for all \mathfrak{p} maximal in $\text{Spec}^\sigma(A)$ and 2.14 implies that $N'_w = 0$. \square

Lemma 2.17 ([6], 6.4). *Let M and N be A -modules and suppose N is generated by $\{n_i\}$. Then every element of $M \otimes_A N$ can be written as $\sum_i m_i \otimes n_i$ with finitely*

many nonzero m_i and $\sum_i m_i \otimes n_i = 0$ in $M \otimes_A N$ if and only if there exist $m'_j \in M$ and $a_{ij} \in A$ such that for every i ,

$$\sum_j a_{ij} m'_j = m_i$$

and for every j ,

$$\sum_i a_{ij} n_i = 0.$$

Proposition 2.18. *Let (M, σ) and (N, σ) be (A, σ) -modules with (N, σ) well-mixed. Then $(M, \sigma) \otimes_{(A, \sigma)} (N, \sigma)$ is well-mixed.*

Proof. Pick a set of generators $\{n_i\}$ for N . Suppose $b \sum_i m_i \otimes n_i = 0$. Then $\sum_i m_i \otimes b n_i = 0$ so 2.17 implies the existence of $m'_j \in M$ and $a_{ij} \in A$ such that for every i , $\sum_j a_{ij} m'_j = m_i$ and for every j , $0 = \sum_i a_{ij} b n_i = b \sum_i a_{ij} n_i$. Since the latter holds in (N, σ) which is well-mixed, we get that $0 = \sigma(b) \sum_i a_{ij} n_i = \sum_i a_{ij} \sigma(b) n_i$. Using 2.17 again, it follows that $\sigma(b) \sum_i m_i \otimes n_i = \sum_i m_i \otimes \sigma(b) n_i = 0$. \square

Proposition 2.19. *Let (M, σ) be a well-mixed (A, σ) -module. The following are equivalent.*

- (1) M is a flat A -module.
- (2) $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$ -module for every $\mathfrak{p} \in \text{Spec}^{\sigma}(A)$.
- (3) $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$ -module for every \mathfrak{p} maximal in $\text{Spec}^{\sigma}(A)$.

Proof. (1) \Rightarrow (2). Assuming (i), it is classically known that $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$ module for every prime \mathfrak{p} . (2) \Rightarrow (3) is trivial.

(3) \Rightarrow (1). Let $(N, \sigma) \rightarrow (P, \sigma)$ be injective. Then $N_{\mathfrak{p}} \rightarrow P_{\mathfrak{p}}$ is injective for every $\mathfrak{p} \in \text{Spec}^{\sigma}(A)$. By assumption, $N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \rightarrow P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ is injective and thus $(N \otimes_A M)_{\mathfrak{p}} \rightarrow (P \otimes_A M)_{\mathfrak{p}}$ is injective for all \mathfrak{p} maximal in $\text{Spec}^{\sigma}(A)$. Since $N \otimes_A M$ is well-mixed by 2.18, Proposition 2.15 implies that $N \otimes_A M \rightarrow P \otimes_A M$ is injective. \square

Remark 2.20. Let $(A, \sigma) \rightarrow (B, \sigma)$ be a homomorphism of well-mixed difference rings such that B is a flat A -module and denote by \bar{A} and \bar{B} the rings of global sections of $\text{Spec}^{\sigma}(A)$ and $\text{Spec}^{\sigma}(B)$. We can consider \bar{B} as an A -module via the morphism $A \hookrightarrow \bar{A} \rightarrow \bar{B}$ as in 3.27, and we can conclude that \bar{B} is flat over A . Indeed, by [19, 3.23(3)], \bar{B} is well-mixed, by [19, 3.23(7)] we know that $\text{Spec}^{\sigma}(B) \simeq \text{Spec}^{\sigma}(\bar{B})$ and $\bar{B}_{\bar{\mathfrak{p}}} \simeq B_{\mathfrak{p}}$, which suffices to apply 2.19.

Proposition 2.21. *Let (A, σ) be a well-mixed domain. If $A_{\mathfrak{p}}$ is normal for every \mathfrak{p} maximal in $\text{Spec}^{\sigma}(A)$, then A is almost normal.*

Proof. Let K be the fraction field of A , let C be the integral closure of A in K and denote by $\phi : A \hookrightarrow C$ the inclusion. By assumption, each $\phi_{\mathfrak{p}}$ is surjective, so 2.16 implies that ϕ is almost surjective and thus $[A]_w = C$. \square

Definition 2.22. A difference scheme (X, Σ) is said to be *normal* if every local ring \mathcal{O}_x , for $x \in X$, is normal.

2.3. Étale morphisms of difference schemes.

Definition 2.23. A morphism $(R, \sigma) \rightarrow (S, \sigma)$ is *formally smooth* (resp. *formally unramified*, *formally étale*), if every solid commutative diagram

$$\begin{array}{ccc} (S, \sigma) & \longrightarrow & A/I \\ \uparrow & \searrow \text{dashed} & \uparrow \\ (R, \sigma) & \longrightarrow & (A, \sigma) \end{array}$$

with I a difference ideal with $I^2 = 0$, there exists at least one (resp. at most one, exactly one) dashed arrow making the diagram commutative.

Recall that a morphism of rings $R \rightarrow S$ is defined to be formally smooth, formally unramified or formally étale by using exactly the same universal property in the category of commutative rings, omitting the difference structure.

Lemma 2.24. *If $(R, \sigma) \rightarrow (S, \sigma)$ is formally smooth, then $R \rightarrow S$ is formally smooth.*

Proof. Let $(P, \sigma) \rightarrow (S, \sigma)$ be a surjective (R, σ) -algebra morphism from a difference polynomial ring P , and let J be the kernel, which is a difference ideal. Consider the above diagram for $A = P/J^2$ and I generated by J . By formal smoothness, we obtain a (difference) morphism $S \rightarrow P/J^2$ which is a right inverse to the surjection $P/J^2 \rightarrow S$, and thus $R \rightarrow S$ is formally smooth using [1, 00TL]. \square

Remark 2.25. For a difference (R, σ) -algebra (S, σ) , the module of relative differentials $\Omega_{S/R}$ naturally classifies R -derivations that commute with σ . Indeed, if we let J be the kernel of the multiplication map $S \otimes_R S \rightarrow S$, it is known that $\Omega_{S/R} \simeq J/J^2$. However, in this context J is a difference ideal and J/J^2 comes equipped with a natural difference structure, which entails in particular that the universal R -derivation $d : S \rightarrow \Omega_{S/R}$ satisfies

$$d\sigma = \sigma d.$$

Remark 2.26. The above is in stark contrast with the various notions of smoothness developed in G. Giabiconi's thesis. With clear intent to apply his theory to the case where σ is a power of the Frobenius automorphism, he postulates $d\sigma = 0$. Another fundamental difference is that étale morphisms in our context as developed below are of relative total dimension 0, whereas in Giabiconi's context they are of relative transformal dimension 0.

Remark 2.27. If (B, σ) is an (A, σ) -algebra of finite σ -type, the second exact sequence for differentials implies that $\Omega_{B/A}$ is a finitely σ -generated (B, σ) -module.

Lemma 2.28. *Given a difference morphism $(R, \sigma) \rightarrow (S, \sigma)$, the following statements are equivalent:*

- (1) $(R, \sigma) \rightarrow (S, \sigma)$ is formally unramified;
- (2) $R \rightarrow S$ is formally unramified;
- (3) $\Omega_{S/R} = 0$.

Proof. In view of 2.25, since $d\sigma = \sigma d$, the classical proof of the equivalence of (2) and (3) also works for the equivalence of (1) and (3). \square

Corollary 2.29. *Let $(R, \sigma) \rightarrow (S, \sigma)$ be a morphism. The following are equivalent:*

- (1) $(R, \sigma) \rightarrow (S, \sigma)$ is almost formally unramified in the sense that $(\Omega_{S/R})_w = 0$;
- (2) for every $\mathfrak{q} \in \text{Spec}^\sigma(S)$ lying over $\mathfrak{p} = \mathfrak{q} \cap R$, $(R_{\mathfrak{p}}, \sigma) \rightarrow (S_{\mathfrak{q}}, \sigma)$ is formally unramified;
- (3) for every $\mathfrak{q} \in \text{Spec}^\sigma(S)$ lying over $\mathfrak{p} = \mathfrak{q} \cap R$, $R_{\mathfrak{p}} \rightarrow S_{\mathfrak{q}}$ is formally unramified.

Proof. Straightforward from 2.14 applied to the (S, σ) -module $\Omega_{S/R}$. \square

Definition 2.30. A morphism $(R, \sigma) \rightarrow (S, \sigma)$ is *smooth* (resp. *unramified*, *étale*), if it is of finite σ -type and formally smooth (resp. formally unramified, formally étale).

Proposition 2.31. *If $(R, \sigma) \rightarrow (S, \sigma)$ is σ -smooth, then $(R, \sigma) \rightarrow (S, \sigma)$ is smooth.*

Proof. It suffices to prove that $(R, \sigma) \rightarrow (S, \sigma)$ is formally smooth. Suppose we have a solid part of the diagram from 2.23. Using the functor $[\sigma]_R$, we produce a diagram

$$\begin{array}{ccccc}
 & & [\sigma]_R S & \longrightarrow & [\sigma]_R A/I \\
 & \nearrow i_S & & \nearrow & \uparrow \\
 (S, \sigma) & \longrightarrow & A/I & & \\
 & \nwarrow & \uparrow & \nwarrow & \uparrow \\
 (R, \sigma) & \longrightarrow & (A, \sigma) & \xleftarrow{\pi_A} & [\sigma]_R A
 \end{array}$$

where the dashed arrow $[\sigma]_R S \rightarrow [\sigma]_R A$ exists by the assumption of σ -smoothness, the morphism π_A exists since A already has a difference structure, and we can construct a morphism $(S, \sigma) \rightarrow (A, \sigma)$ as the obvious composite. \square

Definition 2.32. A morphism $f : (X, \Sigma) \rightarrow (Y, \sigma)$ is called *smooth* (resp. *unramified*, *étale*), if it is of finite transformatal type and for every $x \in X$ and every $\tau \in \Sigma_x$, the morphism $(\mathcal{O}_{f(x)}, \sigma) \rightarrow (\mathcal{O}_x, \tau)$ is smooth (resp. unramified, étale).

Remark 2.33. A morphism $f : (X, \Sigma) \rightarrow (Y, \sigma)$ of finite transformatal type is unramified (resp. étale) if and only if for every $x \in X$ there exists an (affine) open neighbourhood on which f is modelled by an unramified (resp. étale) morphism of difference rings. More precisely, if a morphism $(R, \sigma) \rightarrow (S, \sigma)$ is unramified (resp. étale) at some $\mathfrak{q} \in \text{Spec}^\sigma(S)$ lying over $\mathfrak{p} = \mathfrak{q} \cap R$, then there is a $g \notin \mathfrak{q}$ such that the σ -localisation $(R, \sigma) \rightarrow (S_g, \sigma)$ is unramified (resp. étale).

The above ‘openness’ statement for the property of being unramified is obvious from 2.28 and 2.27. For étaleness, it follows from 2.27 and the *Jacobian criterion* for smoothness which states the following. Let (A, σ) be a difference ring, (B, σ) a formally smooth (A, σ) -algebra, J a reflexive difference ideal of B and let $C = B/J$. Then (C, σ) is a formally smooth (A, σ) -algebra if and only if the natural morphism of difference modules

$$\delta : J/J^2 \rightarrow \Omega_{B/A} \otimes_B C$$

is left-invertible. We omit the details of the proof since these results will not be used in the sequel.

In view of Babbitt's decomposition discussed in the next section, many considerations reduce to a study of unramified or étale morphisms with stronger finiteness assumptions such as quasi-finiteness or finiteness, and we will make every effort to explicitly state them when possible.

Proposition 2.34. *Suppose $(G, \tilde{\Sigma})$ acts admissibly on (X, Σ) of finite transformal type over a difference field (k, σ) and suppose that $(Y, \Sigma_0) = (X, \Sigma)/(G, \tilde{\Sigma})$ and that X is finite over Y . If $G_i(x) = (e)$ for all $x \in X$, the natural projection $(X, \Sigma) \rightarrow (Y, \Sigma_0)$ is finite étale.*

Proof. Since the assertion is local, we may assume that X is affine and that we are in the situation of [19, 4.1]. Suppose $X = \text{Spec}^\Sigma(A)$ and that $(G, \tilde{\Sigma})$ acts on (A, Σ) . By assumption, there is a finite tuple $a \in A$ so that $A = k[a]_\Sigma$. Writing $\bar{a} = \{ga : g \in G\}$, we have that $A = k[\bar{a}]_\sigma$ for any choice of $\sigma \in \Sigma$. Then G acts on each $A_n = k[\bar{a}, \sigma\bar{a}, \dots, \sigma^n\bar{a}]$, and we can form $B_n = A_n^G$. We have $A = \varinjlim_n A_n$ and $B = A^G = \varinjlim_n B_n$ and we have formed a projective limit of Galois covers $p_n : X_n \rightarrow Y_n$ such that $X \rightarrow Y$ is obtained by taking the Σ -fixed points of the ambient Galois covering $\varinjlim_n X_n \rightarrow \varinjlim_n Y_n$. Let $x \in X$ and write x_n for the projection of x in X_n . Since $G_i(x) = (e)$, we have that $G_i(x_n) = (e)$ for all n , so by the known result for Galois covers of locally Noetherian schemes it follows that p_n is étale at x_n . By compatibility of formal étaleness with limits, we conclude that $X \rightarrow Y$ is étale at x . \square

Corollary 2.35. *Suppose (X, Σ) is integral and that $(G, \tilde{\Sigma})$ acts faithfully. Then $X \rightarrow X/G$ is étale if and only if all the inertia groups of elements of X are trivial.*

Proof. By the previous result, it suffices to show that if the quotient morphism is étale at $x \in X$, then $G_i(x) = (e)$. Take an $x \in X$ with $p : X \rightarrow X/G$ étale. We can easily reduce to the case where $G_i(x) = G$ and $\mathbf{k}(x) = \mathbf{k}(p(x))$. Note, since X is integral and G is faithful on X , then G is also faithful on \mathcal{O}_x . However, the classical proof works for the finite local étale extension $\mathcal{O}_{p(x)} \rightarrow \mathcal{O}_x$ and shows that $G = (e)$. \square

2.4. Babbitt's decomposition.

Definition 2.36. A morphism $(S, \sigma) \rightarrow (R, \sigma)$ of integral difference rings is called *benign* if there exists a quasifinite $S \rightarrow R_0$ such that (R, σ) is isomorphic to $[\sigma]_S R_0$ over (S, σ) . In other words, writing $R_{i+1} = R_i \otimes_S S$ for $i \geq 0$ (where the morphism $S \rightarrow S$ is σ), (R, σ) is the (limit) tensor product of the R_i and the canonical morphisms $\sigma_i : R_i \rightarrow R_{i+1}$ over S .

In the *benign Galois* case, R_0 is Galois over S with group G_0 and the Galois group $\text{Gal}(R/S) = \text{Gal}(\mathbf{k}(R)/\mathbf{k}(S)) = (G, ()^\sigma)$ is isomorphic to the direct product of $G_i = \text{Gal}(R_i/S)$ and $()^\sigma$ 'shifts' from G_i to G_{i+1} .

In view of such a specific form of G , for any $h, h' \in G$ there is a $g \in G$ such that $h' = g^{-1}hg^\sigma$, i.e. h and h' are $()^\sigma$ -conjugate, and we get:

Lemma 2.37. *For any $y \in \text{Spec}^\sigma(S)$, any algebraically closed difference field (F, φ) extending $(\mathbf{k}(y), \sigma^y)$, any $\bar{y} \in (S, \sigma)(F, \varphi)$ above y and any $g \in G$, there exists an $\bar{x} \in (R, g\sigma)(F, \varphi)$ lifting \bar{y} .*

Definition 2.38. (1) A morphism $(\psi, ()^\psi) : (S, T) \rightarrow (R, \Sigma)$ of integral almost-strict difference rings is *benign* if for some (or equivalently, for all) $\sigma \in \Sigma$, the morphism $(S, \sigma^\psi) \rightarrow (R, \sigma)$ is benign.

- (2) A morphism $(X, \Sigma) \rightarrow (Y, T)$ of almost-strict difference schemes is *benign* if it is affine and above each open affine subset of Y it is modelled by a fixed-point spectrum of a benign morphism of rings.

An immediate consequence of 2.37 is the following.

Lemma 2.39. *Let $(X, \Sigma) \rightarrow (Y, T)$ be an étale benign Galois morphism. For any $\tau \in T$ and $\sigma \in \Sigma$ mapping to τ , any $y \in Y^\tau$, any algebraically closed difference field (F, φ) extending $(\mathbf{k}(y), \tau^y)$, any $\bar{y} \in Y^\tau(F, \varphi)$ above y , there exists an $\bar{x} \in X^\sigma(F, \varphi)$ lifting \bar{y} .*

Definition 2.40. Two difference schemes (X_1, Σ_1) and (X_2, Σ_2) are called *equivalent*, written $(X_1, \Sigma_1) \simeq (X_2, \Sigma_2)$, if they have isomorphic inversive closures, $(X_1^{\text{inv}}, \Sigma_1^{\text{inv}}) \cong (X_2^{\text{inv}}, \Sigma_2^{\text{inv}})$.

The following is a slight refinement of a fundamental theorem from [3], showing how to use it for not necessarily inversive difference fields.

Lemma 2.41 (Babbitt's Theorem). *Let $(K, \sigma) \rightarrow (L, \sigma)$ be a σ -separable Galois extension of finite σ -type. Then we have a tower*

$$(K, \sigma) \rightarrow (L_0, \sigma) \rightarrow (L_1, \sigma) \rightarrow \cdots \rightarrow (L_n, \sigma) \simeq (L, \sigma)$$

of difference field extensions with L_0/K finite and all L_{i+1}/L_i benign for $i \geq 0$.

Proof. Let us remark that, if F/K is σ -separable, and $F^{\text{inv}} = K^{\text{inv}}(a)_\sigma$ for some $a = a_1, \dots, a_n$, then there is an $r \geq 0$ such that $F = K(\sigma^r a)_\sigma$.

The original theorem from [3] gives that, writing $\tilde{L} = K^{\text{inv}}L$, and \tilde{L}_0 for the core of K^{inv} in \tilde{L} , there exist $u_1, \dots, u_n \in \tilde{L}$ such that $\tilde{L} \simeq \tilde{L}_0(u_1, \dots, u_n)_\sigma$ and for every $0 \leq i \leq n-1$, $\tilde{L}_0(u_1, \dots, u_{i+1})_\sigma$ is a benign extension of $\tilde{L}_0(u_1, \dots, u_i)_\sigma$ with normal minimal generator u_{i+1} .

It is known that \tilde{L}_0 is inversive, so using the above remark for $F = \tilde{L}_0$, we deduce that $\tilde{L}_0 = L_K$, the core of K in L . Bearing in mind that $L \simeq \tilde{L}$, we produce the required decomposition. \square

Babbitt's theorem on algebraic extensions of difference fields has the following consequence in our terminology, providing a deep structure theorem.

Theorem 2.42 (Babbitt's decomposition). *Any generically étale quasi-Galois σ -separable morphism of finite transformatal type $(X, \Sigma) \rightarrow (Y, T)$ of normal affine almost-strict difference schemes factorizes as*

$$(X, \Sigma) \simeq (X_n, \Sigma_n) \rightarrow \cdots \rightarrow (X_1, \Sigma_1) \rightarrow (X_0, \Sigma_0) \rightarrow (Y, T),$$

where $(X_0, \Sigma_0) \rightarrow (Y, T)$ is generically finite étale quasi-Galois and for $i \geq 0$, $(X_{i+1}, \Sigma_{i+1}) \rightarrow (X_i, \Sigma_i)$ is benign Galois. Modulo a transformatal localisation of Y , we can achieve that $(X_0, \Sigma_0) \rightarrow (Y, T)$ is finite étale quasi-Galois, and that $X_{i+1} \rightarrow X_i$ are étale benign Galois.

Proof. By applying Babbitt's theorem 2.41 to the extension of function fields $(\mathbf{k}(Y), \tau) \rightarrow (\mathbf{k}(X), \sigma)$ for a suitable choice of σ and τ we obtain a tower of difference field extensions

$$(\mathbf{k}(Y), \tau) \rightarrow (L_0, \sigma) \rightarrow (L_1, \sigma) \cdots \rightarrow (L_n, \sigma) \simeq (\mathbf{k}(X), \sigma),$$

where $L_0/\mathbf{k}(Y)$ is finite and each $(L_{i+1}, \sigma)/(L_i, \sigma)$ is benign for $i \geq 0$. We let Σ_i be the *Diff*-structure obtained as a restriction of Σ from L_n to L_i . Let (X_i, Σ_i) be the

normalisation of (Y, T) in (L_i, Σ_i) . It is clear from [19, 3.62] that by a transformal localisation we can achieve that $X_0 \rightarrow Y$ is finite étale and it remains to show that each $X_{i+1} \rightarrow X_i$ can be made étale benign, which is granted by the following lemma. \square

Lemma 2.43. *Let (R, σ) be a normal domain with fraction field (K, σ) and let $(K, \sigma) \rightarrow (L, \sigma)$ be a benign extension of difference fields such that L is the composite of the linearly disjoint subfields $L_i = \sigma^i(L_0)$ where L_0 is a fraction field of an étale R -algebra A_0 . Then the normalisation of R in L is the (limit) tensor product of the $A_0^{\sigma^i}$ over R and thus benign over R .*

Proof. Since A_0 is étale over R so is any $A_0^{\sigma^i}$, and any tensor product of those is therefore R -torsion-free and the conclusion follows from linear disjointness in the spirit of the proof of 2.3. \square

Lemma 2.44. *Let $(K, \sigma) \rightarrow (L_0, \sigma) \rightarrow (L_1, \sigma)$ be a tower of Galois extensions of difference fields with L_0/K finite and L_1/L_0 benign. The exact sequence*

$$1 \rightarrow \text{Gal}(L_1/L_0) \rightarrow \text{Gal}(L_1/K) \rightarrow \text{Gal}(L_0/K) \rightarrow 1$$

is split.

Proof. Let us start by using shorthand notation $H = \text{Gal}(L_1/L_0)$, $G = \text{Gal}(L_1/K)$, $G_0 = \text{Gal}(L_0/K)$ and π for the projection $G \rightarrow G_0$. Let us denote by Φ the operator $()^\sigma : G \rightarrow G$. Since L_1/L_0 is benign, H has the specific form of a direct product of infinitely many copies of a finite group and Φ shifts between the copies. Thus we have that $\cap_i \Phi^i H = (1)$. Writing Φ_0 for the operator induced by Φ on G_0 , since G_0 is finite, let us fix some n such that $\Phi_0^n = 1$. The section $s : G_0 \rightarrow G$ is defined by

$$s(g_0) = \cap_i (\Phi^n)^i (\pi^{-1}(g_0)).$$

\square

Lemma 2.45. *Let $(K, \sigma) \rightarrow (L, \tilde{\sigma})$ be a Galois extension of finite $\tilde{\sigma}$ -type. Let $L_0 = L_K$ be the core of K in L . The exact sequence*

$$1 \rightarrow \text{Gal}(L/L_0) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(L_0/K) \rightarrow 1$$

is split.

Proof. Note that the proof of the previous lemma works for an arbitrary L_0/K and a finite subgroup G_0 of $\text{Gal}(L_0/K)$. Using Babbitt's decomposition, let

$$(K, \sigma) \rightarrow (L_0, \sigma) \rightarrow (L_1, \sigma) \cdots \rightarrow (L_n, \sigma) \simeq (L, \sigma),$$

be a tower of difference field extensions with L_0/K finite and all L_{i+1}/L_i benign for $i \geq 0$. Using the previous lemma we can thus inductively 'pull' a copy of $\text{Gal}(L_0/K)$ through the above tower all the way up to $\text{Gal}(L_n/K)$. \square

Definition 2.46. Let $(K, T) \rightarrow (F, \Sigma)$ be an extension of difference fields, and let (L, Σ) be the relative algebraic closure of K in F . We say that an extension $(K, T) \rightarrow (F, \Sigma)$ is a *difference covering* if L/K is Galois and Σ is a finite set of representatives of the isomorphism classes of lifts of all $\tau \in T$ to L .

Proposition 2.47. *Let $(K, \sigma) \rightarrow (F, \tilde{\sigma})$ be a separable difference field extension of finite $\tilde{\sigma}$ -type. Then it can be subsumed in a difference covering, i.e., there exists a difference field extension $(F, \tilde{\sigma}) \rightarrow (\tilde{F}, \tilde{\sigma})$ and an almost strict difference structure $\tilde{\Sigma} \ni \tilde{\sigma}$ on \tilde{F} such that $(K, \sigma) \rightarrow (\tilde{F}, \tilde{\Sigma})$ is a difference covering.*

Proof. Let (L, σ) be the relative algebraic closure of K in F . Let \tilde{L} be its normal closure. Let F' be the fraction field of $F \otimes_K \tilde{L}$. Let $L_0 \subseteq \tilde{L}_0$, be the cores of (K, σ) in L and \tilde{L} , respectively. We apply 2.45 to \tilde{L}/K (resp. \tilde{L}/L) to find a copy of $G = \text{Gal}(\tilde{L}_0/K)$ (resp. $H = \text{Gal}(\tilde{L}_0/L_0)$) in $\text{Gal}(\tilde{L}/K)$ (resp. $\text{Gal}(\tilde{L}/L)$) and set $\tilde{\Sigma} = G\tilde{\sigma}$ (resp. $\Sigma = H\tilde{\sigma}$). It is known that these represent all isomorphism classes of lifts of σ from K to \tilde{L} (resp. from L to \tilde{L}). We obtain difference coverings $(L, \tilde{\sigma}) \rightarrow (\tilde{L}, \Sigma)$ and $(K, \sigma) \rightarrow (\tilde{L}, \tilde{\Sigma})$. To finish, since F' is regular over \tilde{L} , we can lift $\tilde{\Sigma}$ to an extension \tilde{F} of F' by ‘base field extensions’. In more conceptual terms, if we think of F' as a function field of a geometrically irreducible difference scheme X over L , let X_0 be obtained by Weil restriction from \tilde{L} to \tilde{L}^G . Then the base change of X_0 back to \tilde{L} is isomorphic to $\prod_{g \in G} X^g$, which clearly carries a $\tilde{\Sigma}$ -structure and dominates X . \square

Definition 2.48. Let $(X, \Sigma) \rightarrow (Y, T)$ be a generically dominant morphism of integral difference schemes. We shall say that it is a *generic difference covering* if the corresponding inclusion of function fields $(\mathbf{k}(Y), T) \rightarrow (\mathbf{k}(X), \Sigma)$ is a difference covering of fields.

About a half of the proof of 2.47 suffices to deduce the following.

Lemma 2.49. *If $(X, \Sigma) \rightarrow (Y, T)$ is separable algebraic, then it is dominated by the quasi-Galois closure $(\tilde{X}, \tilde{\Sigma}) \rightarrow (Y, T)$ of X over Y , i.e., the (Y, T) -morphism $(\tilde{X}, \tilde{\Sigma}) \rightarrow (X, \Sigma)$ is a generic difference covering.*

Proposition 2.50. *Let $(X, \Sigma) \rightarrow (Y, T)$ be a generically dominant generically smooth morphism of integral normal almost strict difference schemes. Then it can be subsumed in a generic difference covering in the sense of a diagram*

$$\begin{array}{ccc}
 & (\tilde{X}, \tilde{\Sigma}) & \longrightarrow (Z, \Sigma_Z) \\
 & \swarrow \downarrow \searrow & \\
 (X, \Sigma) & & \\
 & \searrow \downarrow \swarrow & \\
 & (Y, T) &
 \end{array}$$

where $(\tilde{X}, \tilde{\Sigma}) \rightarrow (Y, T)$ is the quasi-Galois closure of $(X, \Sigma) \rightarrow (Y, T)$, and $(Z, \Sigma_Z) \rightarrow (Y, T)$ is a generic difference covering.

Proof. In order to simplify notation, let us treat the case of strict difference scheme morphism $(X, \sigma) \rightarrow (Y, \sigma)$. Let L be the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$. As in the proof of 2.47, we may reduce to the case where $L/\mathbf{k}(Y)$ is Galois, and we find a difference structure Σ on L which represents all lifts of σ to the core of $\mathbf{k}(Y)$ in L . Let (\tilde{Y}, Σ) be the normalisation of (Y, σ) in (L, σ) . Our task is to lift the structure Σ to a difference scheme as closely related to (X, σ) as possible. Let $\iota : \{\sigma\} \rightarrow \Sigma$. We construct a Σ -difference scheme $\iota_1(X/\tilde{Y})$ by imitating the definition 3.3 except that the underlying space is the fibre product of copies of X

over \tilde{Y} . Using the universal properties of functors ι^* and $\iota_!$, we obtain a diagram

$$\begin{array}{ccccc}
 & & \iota_!(X/\tilde{Y}) & & \\
 & \nearrow & \downarrow & \nwarrow & \\
 X & \xrightarrow{\quad} & \iota_! X & & \\
 \downarrow & & \downarrow & & \downarrow \\
 & & \tilde{Y} & & \\
 & \nearrow & \downarrow & \nwarrow & \\
 \iota^* \tilde{Y} & \xrightarrow{\quad} & \iota_! \iota^* \tilde{Y} & & \\
 \downarrow & & \downarrow & & \downarrow \\
 Y & \xrightarrow{\quad} & \iota_! Y & &
 \end{array}$$

where the composite $(\iota_!(X/\tilde{Y}), \Sigma) \rightarrow (\tilde{Y}, \Sigma) \rightarrow (Y, \sigma)$ is a generic difference covering. \square

3. BI-FIBERED STRUCTURE OF THE CATEGORY OF DIFFERENCE SCHEMES

Definition 3.1 (Pullback). Let (Y, T) be a difference scheme and let $\psi : \Sigma \rightarrow T$ be a *Diff*-morphism. The *pullback* of Y with respect to ψ is defined as

$$\psi^* Y = \cup_{\sigma \in \Sigma} Y^{\psi(\sigma)},$$

with its induced structure as a Σ -difference scheme, with $\sigma \in \Sigma$ acting as $\psi(\sigma)$ on Y . There is a natural morphism

$$\psi^* Y \rightarrow Y.$$

The following definitions make sense for full difference structures Σ , recall [19, 3.7].

Definition 3.2. Let (X_0, Σ_0) be a difference scheme and let $\iota : \Sigma_0 \hookrightarrow \Sigma$ where Σ has generalised conjugation so that for each $\sigma, \tau \in \Sigma$, there exists a τ' such that ${}^\tau \sigma \tau' \in \Sigma_0$. Let $\tau_i, i \in I$ be the representatives of Σ/Σ_0 , i.e., for each $\sigma \in \Sigma$, and each τ_i , there is a unique τ_j with ${}^{\tau_j} \sigma \tau_i \in \Sigma_0$. The assignment $i \mapsto j$ defines a permutation $\bar{\sigma}$ of I . Consider the space

$$\coprod_{i \in I} X_i,$$

where each X_i is a copy of X_0 (that should be thought of as $\tau_i X_0$) and $\sigma \in \Sigma$ takes X_i to $X_{\bar{\sigma}(i)}$, and acts as ${}^{\tau_{\bar{\sigma}(i)}} \sigma \tau_i$ on the associated copy of X . The underlying space of the (coproduct) pushforward is

$$\iota_* X_0 = \bigcup_{\sigma \in \Sigma} \left(\coprod_{i \in I} X_i \right)^\sigma = \coprod_i \bigcup_{\sigma \tau_i \in \Sigma_0} X_0^{\sigma \tau_i},$$

and the action of Σ is inherited from $\coprod_{i \in I} X_i$.

There is a natural (inclusion) morphism

$$(X_0, \Sigma_0) \rightarrow (\iota_* X_0, \Sigma).$$

Note that $\iota_* X_0$ can be set-wise defined by using just the basic *Diff*-structure on Σ , but the action of Σ requires generalised conjugation.

Definition 3.3. Let (X_0, Σ_0) be a difference scheme and let $\iota : \Sigma_0 \hookrightarrow \Sigma$ and I satisfy the assumptions of 3.2. For $\sigma \in \Sigma$, let $\bar{\sigma}$ denote the permutation of I defined by the requirement that $\bar{\sigma}(i)$ is the unique element of I satisfying

$$\tau_{\bar{\sigma}(i)} \sigma^{\tau_i} \in \Sigma_0.$$

Consider the space

$$\prod_{i \in I} X_i,$$

where each X_i is a copy of X_0 , which can be identified with X_0^I , the space of functions $f : I \rightarrow \coprod_{i \in I} X_i$ with the property $f(i) \in X_i$. We define the action in a natural way with respect to loc. cit.,

$$(\sigma f)(i) = \tau_{\bar{\sigma}(i)} \sigma^{\tau_i} (f(\bar{\sigma}(i))).$$

The underlying space of the (product) pushforward is

$$\iota_! X_0 = \bigcup_{\sigma \in \Sigma} \left(\prod_{i \in I} X_i \right)^\sigma,$$

and the action of Σ is inherited from $\prod_{i \in I} X_i$.

There is a natural (diagonal) morphism

$$(X_0, \Sigma_0) \rightarrow (\iota_! X_0, \Sigma).$$

Definition 3.4. Let (X, Σ) be a difference scheme and let $\pi : \Sigma \rightarrow T$ be a *Diff*-morphism such that there exists a finite group K acting faithfully on Σ such that π can be identified with the canonical projection $\Sigma \rightarrow \Sigma/K = T$. We define

$$\pi_*(X, \Sigma) = (X, \Sigma)/K,$$

considered as a T -difference scheme. There is an obvious quotient morphism

$$(X, \Sigma) \rightarrow (\pi_* X, T).$$

Remark 3.5. Let $\pi : \Sigma \rightarrow T$ be as in 3.4. We shall not need the functor $\pi_!$ in the sequel, but we give an idea of its construction on an affine model. Let (R, Σ) be a difference algebra over a difference field (k, φ) . We let

$$\pi_! R = R_K = k \otimes_{k[K]} R,$$

the ring of K -coinvariants, with its natural T -action. Both natural morphisms $R \rightarrow k \otimes_{k[K]} R$ and $k \otimes_{k[K]} R \rightarrow R$ are used to prove the required adjunction below.

Definition 3.6. Let (X, Σ) be a difference scheme and let $\psi : \Sigma \rightarrow T$ be a *Diff*-morphism which is a composite of *Diff*-morphisms satisfying the requirements of 3.2 or 3.4, $\psi = \psi_1 \circ \dots \circ \psi_n$. We define

$$\psi_* X = \psi_{1*} \dots \psi_{n*} X \quad \text{and} \quad \psi_! X = \psi_{1!} \dots \psi_{n!} X$$

and there are obvious natural morphisms

$$X \rightarrow \psi_* X \quad \text{and} \quad X \rightarrow \psi_! X.$$

Theorem 3.7. Let $\psi : \Sigma \rightarrow T$ be a *Diff*-morphism as in 3.6.

(1) The functor ψ_* is left adjoint to ψ^* , i.e.,

$$\text{Hom}_\Sigma(X, \psi^* Y) \simeq \text{Hom}_T(\psi_* X, Y),$$

functorially in (X, Σ) and (Y, T) .

(2) The functor $\psi_!$ is right adjoint to ψ^* , i.e.,

$$\mathrm{Hom}_\Sigma(\psi^*Y, X) \simeq \mathrm{Hom}_T(Y, \psi_!X),$$

functorially in (X, Σ) and (Y, T) .

Proof. (1) Suppose we have a difference scheme (X, Σ) and let $\iota : \Sigma_0 \hookrightarrow \Sigma$ satisfying the assumptions of 3.2. Writing $(X_0, \Sigma_0) = \iota^*X$ and adopting the notation from loc. cit., there is a natural morphism $\iota_*\iota^*X \rightarrow X$, induced by the morphism $\coprod_i X_i \rightarrow X$, taking the i -th copy of X_0 to $\tau_i(X_0)$. Since $\iota^*\iota_*Y$ is a disjoint union of copies of (Y, Σ_0) , an obvious morphism $(Y, \Sigma_0) \rightarrow \iota^*\iota_*Y$ is the inclusion onto the first copy. This makes it easy to verify that the resulting adjunctions

$$\iota_*\iota^* \rightarrow 1 \quad \text{and} \quad 1 \rightarrow \iota^*\iota_*$$

indeed satisfy the required unit-counit identities for the required adjunction to hold. When $\pi : \Sigma \rightarrow T$ satisfies the requirements of 3.4, $\pi_*\pi^* \rightarrow 1$ is an isomorphism and $1 \rightarrow \pi^*\pi_*$ is essentially the quotient morphism, so the unit-counit relations are easily verified.

(2) With the above notation, a natural morphism $X \rightarrow \iota_!\iota^*X$ is obtained as a restriction of the twisted diagonal embedding $X \rightarrow \prod_i X_i$, where the X_i are copies of X and the morphism is $x \mapsto (\tau_i(x))$. For (Y, Σ_0) , a natural morphism $\iota^*\iota_!Y \rightarrow Y$ is the projection on the first factor, $\iota^*\iota_!Y$ being a direct product of copies of (Y, Σ) . It is just a formality to verify that the resulting adjunctions

$$1 \rightarrow \iota_!\iota^* \quad \text{and} \quad \iota^*\iota_! \rightarrow 1$$

are as required. \square

Remark 3.8. As hinted in [19, 3.5], the functor $(X, \Sigma) \mapsto \Sigma$ makes the category of difference schemes into a (split) fibered category over \mathbf{Diff} .

In Grothendieck's terminology from [12], the existence of left adjoints for the pullback functors makes the category of almost strict difference schemes into a (split) *bi-fibered* category over the category of almost strict difference structures. The author is uncertain on the nomenclature of (split) fibrations in which the pullback functors come with right adjoints as well.

4. EFFECTIVE DIFFERENCE ALGEBRAIC GEOMETRY

As mentioned in the Introduction, one of the main benefits of our Galois stratification procedure is that it makes the *quantifier elimination* and *decision* procedures for fields with Frobenii *effective* in an adequate sense of the word to be expounded in this section.

Ideally, we would like to prove that it makes those procedures *primitive recursive*, which would represent a significant improvement on the known results [16], [4], [13], where it was shown that the decision procedure is recursive.

Unfortunately, due to the underdeveloped state of constructive difference commutative algebra, and the lack of algorithms for relevant operations with difference polynomial ideals, all we can do at the moment is to show that our Galois stratification procedure is primitive recursive reducible to a number of basic operations in difference algebra, which we strongly believe to be primitive recursive themselves.

A ring (R, σ) is said to be *effectively presented*, if it has a finite σ -presentation over \mathbb{Z} , with its generators and relations explicitly given. The following is a list of

elementary operations on effectively presented rings that we shall have recourse to in the sequel.

- (†₁) Given a difference ideal I in a difference polynomial ring over an effectively presented difference field, find its minimal associated σ -primes, i.e., find an irredundant decomposition $\{I\}_\sigma = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ (as in [19, 3.50]).
- (†₂) Given an extension $(K, \sigma) \rightarrow (L, \sigma)$ of effectively presented difference fields of finite σ -type, compute the relative algebraic closure of K in L .
- (†₃) Given an σ -separable Galois extension $(K, \sigma) \rightarrow (L, \sigma)$ of effectively presented difference fields of finite σ -type, compute its Babbitt's decomposition (as in 2.41).
- (†₄) For an effectively presented integrally closed domain (R, σ) with fraction field (K, σ) , and an extension (L, σ) of (K, σ) of finite σ -type, find the integral closure (S, σ) of R in L , and compute the σ -localisation (R', σ) of R so that the corresponding S' is of finite σ -type over R' (cf. 3.62).
- (†₅) Given an effectively presented morphism $f : (R, \sigma) \rightarrow (S, \sigma)$ of effectively presented difference rings and a suitable property P of scheme morphisms, if f is generically σ - P , compute the σ -localisations R' of R and S' of S such that $(R', \sigma) \rightarrow (S', \sigma)$ is σ - P (in particular, we need effective versions of 2.8, 2.9 and 2.10).
- (†₆) Given an algebraic extension $(K, \sigma) \rightarrow (L, \sigma)$ of effectively presented difference fields of finite σ -type, compute the quasi-Galois closure of L over K .
- (†₇) For a finite Galois extension $(K, \sigma) \rightarrow (L, \Sigma)$ of effectively presented difference fields, establish an effective correspondence between the intermediate field extensions and subgroups of the Galois group.
- (†₈) Effective Twisted Lang-Weil estimate. In the situation of [19, 5.2], compute explicitly the constant C and the localisation S' of S .

Definition 4.1. We define \dagger -primitive recursive functions as functions primitive recursive reducible to basic operations in Difference Algebraic Geometry as detailed by the following axioms.

Basic \dagger -primitive recursive functions are:

- (1) *Constant* functions, *Successor* function S , coordinate *Projections*;
- (2) Elementary operations in *difference algebraic geometry* (†₁)–(†₈).

More complex \dagger -primitive recursive functions are built using:

- (3) *Composition*. If f is an n -ary \dagger -primitive recursive function, and g_1, \dots, g_n are m -ary \dagger -primitive recursive function, then

$$h(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$$

is \dagger -primitive recursive.

- (4) *Primitive recursion*. Suppose f is an n -ary and g is an $(n+2)$ -ary \dagger -primitive recursive function. The function h , defined by

$$\begin{aligned} h(0, x_1, \dots, x_n) &= f(x_1, \dots, x_n) \\ h(S(y), x_1, \dots, x_n) &= g(y, h(y, x_1, \dots, x_n), x_1, \dots, x_n) \end{aligned}$$

is \dagger -primitive recursive.

Remark 4.2. The operations (†₅)–(†₈) are primitive recursive.

Proof. In view of the constructive nature of proofs of 2.3, 2.7, 2.8, 2.9, 2.10, the fact that the operation (\dagger_5) is primitive recursive will follow from the existence of the classical primitive recursive procedure for finding a localisation satisfying the property P at the start of the prolongation sequence.

The operation (\dagger_6) is primitive recursive because the construction of quasi-Galois closure is primitive recursive in the algebraic case. Indeed, if $L = K(a_1, \dots, a_n)_\sigma$, and $K(b_1, \dots, b_m)$ is the quasi-Galois closure of $K(a_1, \dots, a_n)$, then $K(b_1, \dots, b_m)_\sigma$ is the quasi-Galois closure of L .

Since the operation (\dagger_7) only deals with finite Galois extensions, it follows that it is primitive recursive by the discussion in [7].

Regarding (\dagger_8) , Hrushovski indicates in the ‘Decidability’ subsection following [13, 13.2] that it is effective, showing how to explicitly compute the constants for the error term. □

Conjecture 4.3. All the operations (\dagger_1) – (\dagger_4) are primitive recursive. The notions of *primitive recursive* and *\dagger -primitive recursive* coincide.

It is plausible to the author that the relevant operations in difference algebra will be shown to be primitive recursive in the near future. Consequently, our Galois stratification, as well as the decision procedure for fields with Frobenii will be shown to be primitive recursive.

5. GALOIS STRATIFICATION

5.1. Galois stratifications and Galois formulae.

Definition 5.1. Let (X, σ) be an (S, σ) -difference scheme. It is often useful to consider its *realisation functor* \tilde{X} . For each $s \in S$ and each algebraically closed difference field (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$\tilde{X}(s, (F, \varphi)) = X_s(F, \varphi).$$

An (S, σ) -*subassignment* of X is any subfunctor \mathcal{F} of \tilde{X} . Namely, for any $(s, (F, \varphi))$ as above,

$$\mathcal{F}(s, (F, \varphi)) \subseteq X_s(F, \varphi),$$

and for any $u : (s, (F, \varphi)) \rightarrow (s', (F', \varphi'))$, $\mathcal{F}(u)$ is the restriction of $\tilde{X}(u)$ to $\mathcal{F}(s, (F, \varphi))$.

Definition 5.2. Let (S, σ) be a difference scheme and let (X, σ) be a difference scheme over (S, σ) . A *normal (twisted) Galois stratification*

$$\mathcal{A} = \langle X, Z_i/X_i, C_i \mid i \in I \rangle$$

of (X, σ) over (S, σ) is a partition of (X, σ) into a finite set of integral normal σ -locally closed difference (S, σ) -subvarieties (X_i, σ) of (X, σ) , each equipped with a connected Galois covering $(Z_i, \Sigma_i)/(X_i, \sigma)$ with group $(G_i, \tilde{\Sigma}_i)$, and C_i is a ‘conjugacy domain’ in Σ_i , as in [19, Section 4].

A normal Galois stratification is *effectively given*, if the base (S, σ) and all the pieces Z_i , X_i are affine with effectively presented coordinate rings (i.e., of finite σ -presentation over \mathbb{Z}).

Definition 5.3. We define the (*twisted*) *Galois formula* over (S, σ) associated with the above stratification \mathcal{A} to be its realisation subassignment $\tilde{\mathcal{A}}$ of X . Given a point $s \in S$ and an algebraically closed difference field (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$\tilde{\mathcal{A}}(s, (F, \varphi)) = \mathcal{A}_s(F, \varphi) = \bigcup_i \{x \in X_{i,s}(F, \varphi) \mid \varphi_x^{Z_i/X_i} \subseteq C_i\},$$

where $\varphi_x^{Z_i/X_i}$ denotes the local φ -substitution at x , as defined in [19, Subsection 4.2].

It can be beneficial to think of the Galois formula associated with \mathcal{A} and a given *parameter* $s \in S$ as of the formal expression

$$\theta(t; s) \equiv \{t \in X_s \mid \text{ar}(t) \subseteq \text{con}(\mathcal{A})\},$$

whose *interpretation* in any given (F, φ) extending $(\mathbf{k}(s), \sigma^s)$ is given above. Namely, the ‘Artin symbol’ $\text{ar}(t)$ of a point $x \in X_{i,s}(F, \varphi)$ is interpreted as $\text{ar}(x) = \varphi_x$, the local φ -substitution at x with respect to the covering Z_i/X_i , and $\text{con}(\mathcal{A})$ at x becomes the appropriate C_i .

Remark 5.4. If we fix a lift $\sigma_i \in \Sigma_i$ of σ for each i , the above data is equivalent to fixing for each i a $()^{\sigma_i}$ -conjugacy domain \dot{C}_i in G_i , i.e., a union of $()^{\sigma_i}$ -conjugacy classes in G_i . This justifies the adjective ‘twisted’ used alongside ‘stratification’. Clearly,

$$\mathcal{A}_s(F, \varphi) = \bigcup_i \{x \in X_{i,s}(F, \varphi) \mid \varphi_x^{Z_i/X_i} \in \dot{C}_i\}.$$

Remark 5.5. In view of our previous consideration of constructible functions on (X, σ) , it is clear that a constructible function has only finitely many values and that Galois formulae arise as ‘level-sets’ of constructible functions. In fact, by identifying a conjugacy domain C with its characteristic function 1_C , we can think of a Galois formula associated with

$$\mathcal{A} = \langle X, Z_i/X_i, C_i \mid i \in I \rangle$$

as the preimage $1_{\mathcal{A}}^{-1}(1)$ of the constructible function

$$1_{\mathcal{A}} = \langle X, Z_i/X_i, 1_{C_i} \mid i \in I \rangle.$$

Alternatively, $1_{\mathcal{A}}$ can be thought of as a characteristic function of \mathcal{A} on X . With this duality in mind, starting from the *Boolean ring* of characteristic functions of Galois formulae on X (which is the subring of idempotents in the algebra $\mathcal{C}(X)$ of all constructible functions, see [19, 5.22]), we can define a *Boolean algebra* structure on the class (really a set) of Galois formulae on a given difference scheme (X, σ) over (S, σ) :

- (1) $0_X = \langle X, X/X, 0 \rangle$, $1_X = \langle X, X/X, 1 \rangle$;
- (2) $1_{\mathcal{A} \wedge \mathcal{B}} = 1_{\mathcal{A}} \cdot 1_{\mathcal{B}}$;
- (3) $1_{\mathcal{A} \vee \mathcal{B}} = 1_{\mathcal{A}} + 1_{\mathcal{B}} - 1_{\mathcal{A}} \cdot 1_{\mathcal{B}}$;
- (4) $1_{\neg \mathcal{A}} = 1_X - 1_{\mathcal{A}}$.

Although efficient, the above definition of the Boolean algebra structure on Galois formulae on a given difference scheme can be made more explicit and informative as follows.

Definition 5.6. Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be an (S, φ) -morphism, let $\mathcal{A} = \langle X, Z_i/X_i, C_i \rangle$ be an (S, σ) -Galois stratification on X and let $\mathcal{B} = \langle Y, W_j/Y_j, D_j \rangle$ be an (S, σ) -Galois stratification on Y .

- (1) With notation of [19, 5.16], the *inflation* of \mathcal{A} is defined as

$$\mathcal{A}' = \langle X, Z'_i/X_i, \pi_i^{-1}(C_i) \rangle,$$

and has the property that for every $s \in S$, and every algebraically closed (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$\mathcal{A}'_s(F, \varphi) = \mathcal{A}_s(F, \varphi).$$

- (2) With notation of [19, 5.18], the *refinement* of \mathcal{A} is defined as

$$\mathcal{A}' = \langle X, Z_{ij}/X_{ij}, \iota_{ij}^{-1}(C_i) \rangle,$$

and has the property that for every $s \in S$, and every algebraically closed (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$\mathcal{A}'_s(F, \varphi) = \mathcal{A}_s(F, \varphi).$$

- (3) With notation of [19, 5.20], the *pullback* $f^*\mathcal{B}$ of \mathcal{B} with respect to f is defined as a refinement of

$$\langle X, Z_j/X_j, \iota_j^{-1}(D_j) \rangle$$

to a normal refinement of the stratification X_j of X . It has the property that for every $s \in S$, and every algebraically closed (F, φ) extending $(\mathbf{k}(s), \sigma^s)$,

$$f^*\mathcal{B}_s(F, \varphi) = f_s^{-1}(\mathcal{B}_s(F, \varphi)).$$

Definition 5.7. Let (X, σ) be an (S, σ) -difference scheme. The class of (S, σ) -Galois formulae on X has a *Boolean algebra* structure as follows.

- (1) $\perp_X = \langle X, X/X, \emptyset \rangle$, $\top_X = \langle X, X/X, \{\sigma\} \rangle$.

For Galois formulae on X given by \mathcal{A} and \mathcal{B} , upon a refinement and an inflation we may assume that $\mathcal{A} = \langle X, Z_i/X_i, C_i \rangle$ and $\mathcal{B} = \langle X, Z_i/X_i, D_i \rangle$, with $C_i, D_i \subseteq \Sigma_i$.

- (2) $\mathcal{A} \wedge \mathcal{B} = \langle X, Z_i/X_i, C_i \cap D_i \rangle$.
(3) $\mathcal{A} \vee \mathcal{B} = \langle X, Z_i/X_i, C_i \cup D_i \rangle$.
(4) $\neg \mathcal{A} = \langle X, Z_i/X_i, \Sigma_i \setminus C_i \rangle$.

5.2. Direct Image Theorems. The following result can be considered as a difference version of Chevalley's theorem stating that a direct image of a constructible set by a scheme morphism of finite presentation is again constructible.

Proposition 5.8. *Let $f : (X, \Sigma) \rightarrow (Y, T)$ be a generic difference covering of finite transformatal type. Then $f(X)$ contains a dense open subset of Y . If f is effectively presented, we can compute it in a \dagger -primitive recursive way.*

Proof. It is enough to consider the case when $T = \{\sigma\}$. By σ -localising (2.8), we may assume that f is a σ -smooth morphism between normal difference schemes. This is \dagger -primitive recursive by (\dagger_8) . By considering the normalisation \tilde{Y} in the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$, we obtain a baby Stein factorisation $(X, \Sigma) \rightarrow (\tilde{Y}, \Sigma) \rightarrow (Y, \sigma)$, where the first map has generically geometrically integral fibres, and the second is generically σ -étale with $\mathbf{k}(\tilde{Y})/\mathbf{k}(Y)$ Galois. By localising further using 2.9, we may assume that all the fibres of the first morphism are non-empty so the first morphism is surjective, and we can restrict our attention to the second morphism. These steps are \dagger -primitive recursive by (\dagger_2) , (\dagger_4) , (\dagger_5) .

Using 2.8, by another localisation we restrict to the case where $(\tilde{Y}, \Sigma) \rightarrow (Y, \sigma)$ is σ -étale. Applying Babbitt's decomposition 2.42 to $(\tilde{Y}, \Sigma) \rightarrow (Y, \sigma)$ and a further localisation if necessary, we obtain a tower

$$\tilde{Y} \simeq Y_n \rightarrow \cdots \rightarrow Y_1 \rightarrow Y_0 \rightarrow Y,$$

with $(Y_0, \Sigma) \rightarrow (Y, \sigma)$ finite Galois and all $Y_{i+1} \rightarrow Y_i$ benign, for $i \geq 0$. In the effective case, all this can be achieved in a \dagger -primitive recursive way, using (\dagger_5) , (\dagger_3) , (\dagger_4) . The first morphism is a Galois covering and therefore surjective by [19, 4.1] and its generalisations, and benign morphisms are clearly surjective. Thus, we conclude that f can be made surjective upon a finite σ -localisation, which is enough to deduce the required statement. \square

Definition 5.9. Let (S, σ) be a normal integral difference scheme of finite σ -type over \mathbb{Z} , and let (X, σ) be an (S, σ) -difference scheme. Let \mathcal{F} and \mathcal{F}' be (S, σ) -subassignments of X . We shall say that \mathcal{F} and \mathcal{F}' are *equivalent with respect to fields with Frobenii* over S and write

$$\mathcal{F} \equiv_S \mathcal{F}',$$

if for every closed $s \in S$, every sufficiently large finite field k with (\bar{k}, φ_k) extending $(\mathbf{k}(s), \sigma^s)$,

$$\mathcal{F}(s, (\bar{k}, \varphi_k)) = \mathcal{F}'(s, (\bar{k}, \varphi_k)).$$

Definition 5.10. Let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of (S, σ) -difference schemes and let \mathcal{A} be Galois stratification on X , associated with a Galois formula $\chi(x; s) \equiv \{x \in X_s \mid \text{ar}(x) \subseteq \text{con}(\mathcal{A})\}$. For $s \in S$ and (F, φ) an algebraically closed difference field extending $(\mathbf{k}(s), \sigma^s)$, we define a subassignment $f_{\exists} \mathcal{A}$ of Y by the rule

$$f_{\exists} \mathcal{A}(s, (F, \varphi)) = (f_{\exists} \mathcal{A})_s(F, \varphi) = f_s(\mathcal{A}_s(F, \varphi)) \subseteq Y_s(F, \varphi).$$

It can also be considered as an expression

$$v(y; s) \equiv \{y \in Y_s \mid \exists x \chi(x; s), f_s(x) = y\}$$

which justifies the notation somewhat.

Lemma 5.11. Suppose $(Z, \Sigma_Z) \rightarrow (X, \Sigma_X) \rightarrow (Y, \sigma)$ is a tower of étale Galois coverings, and let $C \subseteq \Sigma_Z$ be a conjugacy domain. We have an exact sequence of groups with operators

$$1 \rightarrow \text{Gal}(Z/X) \rightarrow \text{Gal}(Z/Y) \rightarrow \text{Gal}(X/Y) \rightarrow 1.$$

Then

$$f_{\exists} \langle Z/X, C \rangle = \langle Z/Y, C \rangle^{\sim}.$$

Apart from the subtlety that the short exact sequence is needed to deduce that C remains a conjugacy domain with respect to the covering Z/Y , the proof is quite obvious.

Lemma 5.12. Let $(Z, \Sigma_Z) \rightarrow (X, \Sigma_X) \rightarrow (Y, \sigma)$ be a tower of étale Galois coverings, and assume that $\iota : \Sigma_0 \hookrightarrow \Sigma$ is a Diff-morphism satisfying the conditions

from 3.2. Let $(X_0, \Sigma_{X_0}) = \iota^*(X, \Sigma)$, suppose that (Z_0, Σ_{Z_0}) makes the square in the diagram

$$\begin{array}{ccc} Z_0 & \longrightarrow & Z \\ \downarrow & & \downarrow \\ X_0 & \xrightarrow{(i, \iota)} & X \\ f_0 \downarrow & \swarrow f & \\ Y & & \end{array}$$

Cartesian, and let C_0 be a conjugacy domain in Σ_{Z_0} . Then

$$f_{0\exists} \langle Z_0/X_0, C_0 \rangle = f_{\exists i\exists} \langle Z_0/X_0, C_0 \rangle = f_{\exists} \langle Z/X, \iota_* C_0 \rangle,$$

where $\iota_* C_0$ is the smallest conjugacy domain in Σ_Z containing $\iota(C_0)$.

Proof. Note that an f -fibre of $i_{\exists} \langle Z_0/X_0, C_0 \rangle$ is one of the blocks of an f -fibre of $\langle Z/X, \iota_* C_0 \rangle$ which are in bijective correspondence with the different conjugates of C_0 contained in $\iota_* C_0$. Thus the f_{\exists} -images are equal. \square

The main result of this paper is that the class of Galois formulae over fields with Frobenii is closed under taking images by f_{\exists} . More precisely, we have the following.

Theorem 5.13. *Let (S, σ) be a difference scheme of finite σ -type over \mathbb{Z} and let $f : (X, \sigma) \rightarrow (Y, \sigma)$ be a morphism of (S, σ) -difference schemes of finite σ -type. For every Galois formula \mathcal{A} of X , the subassignment $f_{\exists} \mathcal{A}$ is \equiv_S -equivalent to a Galois formula on Y , i.e., there exists a Galois formula \mathcal{B} on Y such that*

$$f_{\exists} \mathcal{A} \equiv_S \mathcal{B}.$$

When \mathcal{A} is effectively given, a \dagger -primitive recursive procedure yields an effectively given \mathcal{B} and a constant $m > 0$ such that for each closed $s \in S$ and each finite field k with $|k| \geq m$ with (\bar{k}, φ_k) extending $(\mathbf{k}(s), \sigma^s)$,

$$(f_{\exists} \mathcal{A})_s(\bar{k}, \varphi_k) = f_s(\mathcal{A}_s(\bar{k}, \varphi_k)) = \mathcal{B}_s(\bar{k}, \varphi_k).$$

Proof. The proof is by devissage, whereby in each step we calculate the direct image on a dense open piece and postpone the calculation on the complement to the next step. At the end of the procedure, we will have obtained the image of each piece of the domain as a Galois stratification supported on a locally closed piece of the codomain. To finish, we extend all of these trivially to produce Galois formulae on the whole of Y , and we take their disjunction to represent the total image as a Galois formula.

It is straightforward to reduce to the case where X and Y are integral, using (\dagger_1) . Moreover, the case when f is purely inseparable or purely σ -inseparable is easily resolved.

Thus, by a noetherian induction trick using generic σ -smoothness 2.8 and 5.8, after a possible refinement of \mathcal{A} , we obtain stratifications X_i and Y_j into integral normal locally closed (S, σ) -subschemes of X and Y such that for every i there exists a j with $f(X_i) \subseteq Y_j$ and $f_i := f|_{X_i} : (X_i, \sigma) \rightarrow (Y_j, \sigma)$ is σ -smooth. This can be done in a \dagger -primitive recursive way, using (\dagger_5) and the effective case of 5.8.

By the philosophy of the proof, we can restrict our attention to one of the f_i , so we disregard the index i and write $f : (X, \sigma) \rightarrow (Y, \sigma)$ in place of f_i , and we may

assume that \mathcal{A} on X is basic, $\mathcal{A} = \langle Z/X, C \rangle$, where $(Z, \Sigma_Z)/(X, \sigma)$ is a connected Galois covering with group $(G, \tilde{\Sigma}_Z)$ and C is a G -conjugacy domain in Σ_Z .

By considering the normalisation \tilde{Y} in the relative algebraic closure of $\mathbf{k}(Y)$ inside $\mathbf{k}(X)$, we obtain a baby Stein factorisation $(X, \sigma) \rightarrow (\tilde{Y}, \sigma) \rightarrow (Y, \sigma)$, where the first morphism has generically geometrically integral fibres, and the second is generically σ -étale. By a further localisation, using 2.9 and 2.8 and 5.8 we can assume the first morphism has connected fibres and the second is σ -étale. All of this is \dagger -primitive recursive by (\dagger_4) , (\dagger_2) , (\dagger_5) . Thus, we can split our considerations into two cases.

Case 1: f has geometrically integral fibres.

The proof of this case can be extrapolated from [19, 5.28] for finite-dimensional schemes, but now we have to treat a general case. We give a direct proof, following analogous signposts.

Let (W, Σ_W) be the normalisation of (Y, σ) in the relative algebraic closure of $\mathbf{k}(Y)$ in $(\mathbf{k}(Z), \Sigma_Z)$, in the effective case calculated by (\dagger_2) and (\dagger_4) . Then (W, Σ_W) is a Galois cover of (Y, σ) . Writing $(X_W, \Sigma_{X_W}) = (X, \sigma) \times_{(Y, \sigma)} (W, \Sigma_W)$, we obtain an exact sequence

$$(1) \quad 1 \rightarrow \text{Gal}(Z/X_W) \rightarrow \text{Gal}(Z/X) \rightarrow \text{Gal}(W/Y) \rightarrow 1,$$

together with a *Diff*-quotient morphism

$$\pi : \Sigma_Z \rightarrow \Sigma_Z / \text{Gal}(Z/X_W) = \Sigma_W.$$

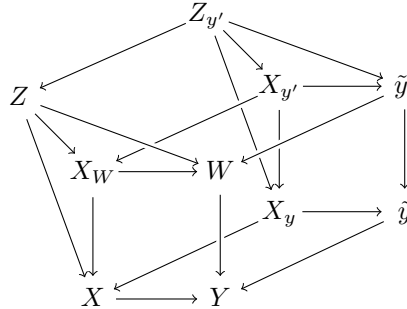
Let $D = \pi_*(C)$ be the image of C in Σ_W , computed by (\dagger_7) , and we claim that

$$f_{\exists} \langle Z/X, C \rangle = \langle W/Y, D \rangle,$$

i.e., for all closed $s \in S$, all large enough k with (\bar{k}, φ_k) extending $(\mathbf{k}(s), \sigma^s)$,

$$(2) \quad \begin{aligned} & \{y \in Y_s(\bar{k}, \varphi_k) \mid \exists x \in X_s(\bar{k}, \varphi_k), \varphi_{k,x} \in C, f_s(x) = y\} \\ &= \{y \in Y_s(\bar{k}, \varphi_k) \mid \varphi_{k,y} \in D\}. \end{aligned}$$

A routine verification of the left to right inclusion needs no assumptions on the size of k . Conversely, let $\bar{y} \in Y_s(\bar{k}, \varphi_k)$, $\varphi_{k,\bar{y}} = D_0 \subseteq D$. Pick some \bar{y}' in the fibre of W/Y above \bar{y} with $\varphi_{k,\bar{y}'} \in D_0$. Let us denote by $y \in Y_s$ and $y' \in W_s$ the loci of \bar{y} and \bar{y}' , $\tilde{y} = \text{Spec}^{\sigma^y}(\mathbf{k}(y))$, $\tilde{y}' = \text{Spec}^{\Sigma^{y'}}(\mathbf{k}(y'))$ (where $\Sigma^{y'}$ is shorthand for $\Sigma_W^{y'}$) and consider the diagram



where $(X_y, \sigma_y) = (X, \sigma) \times_{(Y, \sigma)} (\tilde{y}, \sigma^y)$ is the fibre of X above y , $(X_{y'}, \Sigma_{y'}) = (X_W, \Sigma_{X_W}) \times_{(W, \Sigma_W)} (\tilde{y}', \Sigma^{y'})$ is the fibre of X_W above y' , and

$$(Z_{y'}, \Sigma_{y'}) = (Z, \Sigma_Z) \times_{(X_W, \Sigma_{X_W})} (X_{y'}, \Sigma_{y'}) = (Z, \Sigma_Z) \times_{(W, \Sigma_W)} (\tilde{y}', \Sigma^{y'})$$

is the fibre of Z above y' . By construction, $Z \rightarrow W$ has geometrically connected fibres so we conclude that $Z_{y'}$ is geometrically connected and $\text{Gal}(Z_{y'}/X_{y'}) \cong \text{Gal}(Z/X \times_Y W)$. In the diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(Z_{y'}/X_{y'}) & \longrightarrow & \text{Gal}(Z_{y'}/X_y) & \longrightarrow & \text{Gal}(\tilde{y}'/\tilde{y}) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \text{Gal}(Z/X_W) & \longrightarrow & \text{Gal}(Z/X) & \longrightarrow & \text{Gal}(W/Y) \longrightarrow 1 \end{array}$$

the left vertical arrow is an isomorphism and $\text{Gal}(\tilde{y}'/\tilde{y}) = \text{Gal}(\mathbf{k}(y')/\mathbf{k}(y))$. It follows that $\text{Gal}(Z_{y'}/X_y) = \text{Gal}(Z/X) \times_{\text{Gal}(W/Y)} \text{Gal}(\tilde{y}'/\tilde{y})$ and we get a Cartesian diagram of difference structures:

$$\begin{array}{ccc} & \Sigma_{y'} & \\ \swarrow & & \searrow \\ \Sigma_Z & & \Sigma^{y'} \\ \searrow & & \swarrow \\ & \Sigma_W & \end{array}$$

Thus we can find a conjugacy domain $C' \subseteq \Sigma_{y'}$ which maps into C in Σ_Z (and eventually to $D_0 \subseteq \Sigma_W$), as well as onto φ_k . It suffices to find an $x \in X_y(\bar{k}, \varphi_k)$ with $\varphi_{k,x} \subseteq C'$ with respect to the cover $Z_{y'}/X_y$, and this is possible for large enough k by Twisted Chebotarev [19, 5.30]. The relevant bound for the size of k can be calculated by (\dagger_8) .

Case 2: f is σ -étale. Using 2.49, modulo a σ -localisation, we may assume that the quasi-Galois closure $h : (\tilde{X}, \tilde{\Sigma}) \rightarrow (Y, \sigma)$ of X over Y strictly dominates $f : (X, \sigma) \rightarrow (Y, \sigma)$, i.e., that the morphism $r : (\tilde{X}, \tilde{\Sigma}) \rightarrow (X, \sigma)$ is surjective. Then

$$f_{\exists} \mathcal{A} = f_{\exists} r_{\exists} r^* \mathcal{A} = h_{\exists} r^* \mathcal{A},$$

so it is enough to show that the direct image by h_{\exists} of a Galois formula is again Galois. In the effective case, we can do this via (\dagger_6) .

In other words, we may assume that $f : (X, \Sigma) \rightarrow (Y, \sigma)$ is σ -étale quasi-Galois, so we can benefit from Babbitt's decomposition. Indeed, modulo a localisation, 2.42 yields a decomposition of f as

$$(X, \Sigma) \simeq (X_n, \Sigma_n) \rightarrow \cdots \rightarrow (X_1, \Sigma_1) \rightarrow (X_0, \Sigma_0) \rightarrow (Y, \sigma),$$

with $(X_0, \Sigma_0) \rightarrow (Y, \sigma)$ finite étale quasi-Galois, and for $i \geq 0$, $(X_{i+1}, \Sigma_{i+1}) \rightarrow (X_i, \Sigma_i)$ étale benign Galois. This can be achieved in a \dagger -primitive recursive way by using (\dagger_3) and (\dagger_4) . We can reduce to two subcases as follows.

Case 2(a): $f_0 : (X_0, \Sigma_0) \rightarrow (Y, \sigma)$ is finite étale quasi-Galois. We are given a Galois covering $(Z_0, \Sigma_{Z_0}) \rightarrow (X, \Sigma_0)$ and a conjugacy class C_0 in Σ_{Z_0} . Thus $(Z_0, \Sigma_{Z_0}) \rightarrow (Y, \sigma)$ is quasi-Galois so it is subsumed in a Galois covering $(Z, \Sigma_Z) \rightarrow (Y, \sigma)$ which is obtained by essentially just expanding the difference structure via $\iota_Z : \Sigma_{Z_0} \rightarrow \Sigma_Z$ so that $Z_0 = \iota_Z^* Z$ and we can apply 5.12 and 5.11 to obtain

$$f_{0\exists} \langle Z_0/X_0, C_0 \rangle = f_{\exists} \langle Z/X, \iota_* C_0 \rangle = \langle Z/Y, \iota_* C_0 \rangle.$$

The relevant calculations in the effective case are performed using (\dagger_6) and (\dagger_7) .

Case 2(b): $f : (X, \Sigma) \rightarrow (Y, T)$ is benign étale quasi-Galois. We are given a Galois covering $(Z, \Sigma_Z) \rightarrow (X, \Sigma)$ and a conjugacy domain C in Σ_Z . Babbitt's

decomposition 2.42 applied to Z/Y yields a sequence

$$(Z, \Sigma_Z) \simeq (Z_n, \Sigma_n) \rightarrow \cdots \rightarrow (Z_1, \Sigma_1) \rightarrow (Z_0, \Sigma_0) = (W, \Sigma_W) \rightarrow (Y, T)$$

where $(W, \Sigma_W)/(Y, T)$ can be assumed to be a finite étale Galois covering and Z_{i+1}/Z_i is benign for $i \geq 0$. Since $\mathbf{k}(X)$ is linearly disjoint from $\mathbf{k}(W)$ over $\mathbf{k}(Y)$, we obtain an exact sequence of the form (1) again, and we have the corresponding *Diff*-morphism $\pi : \Sigma_Z \rightarrow \Sigma_Z/\text{Gal}(Z/X_W) = \Sigma_W$. Let $D = \pi_* C$ be the image of C in Σ_W , and we claim that (2) holds for any s closed in S and k and (k, φ_k) extending $(\mathbf{k}(s), \varphi_s)$. To see the non-trivial inclusion, let y be an element of the right hand side and let $z_0 \in W = Z_0$ such that $z_0 \mapsto y$ and $\varphi_{k, z_0} \in D$. Using the property 2.39 repeatedly, we can lift z_0 through the ‘stack’ of benign extensions Z_{i+1}/Z_i to a point $z \in Z^{\tilde{\sigma}}(k, \varphi_k)$ with $\tilde{\sigma} \in C$, and then the image x of z in X_s has the properties $\varphi_{k, x} \sim \tilde{\sigma} \in C$ and $f(x) = y$. This case is \dagger -primitive recursive by $(\dagger_2), (\dagger_4), (\dagger_7)$.

Corollary 5.14. *With assumptions of 5.13, it makes sense to define a subassignment*

$$f_{\forall} \mathcal{A} = \neg f_{\exists}(\neg \mathcal{A}),$$

and it is again a Galois formula on Y .

5.3. Quantifier elimination for Galois formulae. Let (R, σ) be an integral normal difference ring of finite σ -type over \mathbb{Z} , and let $(S, \sigma) = \text{Spec}^{\sigma}(R)$.

Definition 5.15. (1) A *first-order formula* over (S, σ) is a first-order expression built in the usual way starting from terms which are difference polynomials with coefficients in (R, σ) . If x_1, \dots, x_n are the free variables of a formula θ , and $r_1, \dots, r_m \in R$ are all the coefficients of all polynomials appearing as terms of θ , we can express this dependence by writing

$$\theta(x_1, \dots, x_n; r_1, \dots, r_n),$$

where the r_i are thought of as *parameters* of θ .

- (2) An (R, σ) -formula $\theta(x_1, \dots, x_n; r_1, \dots, r_n)$ gives rise to a subassignment $\tilde{\theta}$ of $\mathbb{A}_{(S, \sigma)}^n$ by the following procedure. Let $s \in S$, and let (F, φ) be an algebraically closed difference field extending $(\mathbf{k}(s), \varphi^s)$. Taking the images of the r_i by the composite

$$(R, \sigma) \rightarrow (\mathcal{O}_{S, s}, \sigma_s^{\sharp}) \rightarrow (\mathbf{k}(s), \sigma^s) \rightarrow (F, \varphi),$$

we obtain a honest first-order formula in the language of difference rings on the field (F, φ) , and we take its set of realisations to be the value

$$\tilde{\theta}(s, (F, \varphi)) \subseteq \mathbb{A}_s^n(F, \varphi).$$

- (3) An (S, σ) -subassignment \mathcal{F} of \mathbb{A}_S^n is called *definable* if there exists a first-order formula $\theta(x_1, \dots, x_n)$ over (R, σ) such that $\mathcal{F} = \tilde{\theta}$.

Theorem 5.16 (Quantifier elimination for fields with Frobenii). *The class of definable (S, σ) -subassignments is equal to the class of (S, σ) -Galois formulae modulo the relation \equiv_S , i.e., with respect to fields with Frobenii over S . The quantifier elimination procedure is \dagger -primitive recursive.*

Proof. Let us show by induction on the complexity of a first-order formula that every (S, σ) -formula in the language of rings $\theta(x_1, \dots, x_n)$ is equivalent to a Galois formula on $\mathbb{A}_{(S, \sigma)}^n$.

- (1) If $\theta(x_1, \dots, x_n)$ is a positive atomic formula, it is given by a difference-polynomial equation $P(x_1, \dots, x_n) = 0$, which cuts out a closed difference subscheme Z of $\mathbb{A}_{(S, \sigma)}^n$. We can stratify the affine space into normal locally closed pieces X_i such that each piece is either completely in Z or in its complement. For each X_i , we choose a trivial Galois covering $(X_i, \sigma) \rightarrow (X_i, \sigma)$, and we let $C_i = \{\sigma\}$ when $X_i \subseteq Z$, and $C_i = \emptyset$ otherwise. Then $\mathcal{A} = \langle \mathbb{A}_S^n, X_i/X_i, C_i \rangle$ has the property that

$$\tilde{\theta} = \tilde{\mathcal{A}}.$$

- (2) If $\theta(\bar{x}) = \theta_1(\bar{x}_1) \wedge \theta_2(\bar{x}_2)$, where it is assumed that \bar{x} is the union of variables in \bar{x}_1 and \bar{x}_2 , we choose the corresponding projections $p_i : \mathbb{A}^{|\bar{x}|} \rightarrow \mathbb{A}^{|\bar{x}_i|}$. By induction hypothesis, we can find Galois formulae \mathcal{A}_i on $\mathbb{A}^{|\bar{x}_i|}$ such that $\theta_i \equiv_S \mathcal{A}_i$. Then

$$\theta \equiv_S p_1^* \mathcal{A}_1 \wedge p_2^* \mathcal{A}_2.$$

- (3) If $\theta = \theta_1 \vee \theta_2$, we proceed analogously to the previous step.

- (4) If $\theta = \neg \theta'$, and $\theta' \equiv_S \mathcal{A}$, then

$$\theta \equiv_S \neg \mathcal{A}.$$

- (5) If $\theta(x_2, \dots, x_n) = \exists x_1 \theta'(x_1, x_2, \dots, x_n)$, and $\theta' \equiv_S \mathcal{A}$ on \mathbb{A}^n , writing x_1 for the projection $\mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$ to the variables x_2, \dots, x_n , we have that

$$\theta \equiv_S \exists x_1 \theta' \equiv_S x_{1\exists} \mathcal{A},$$

which is Galois by 5.13.

- (6) If $\theta = \forall x_1 \theta'$, and $\theta' \equiv_S \mathcal{A}$, then

$$\theta \equiv_S \forall x_1 \theta' \equiv_S x_{1\forall} \mathcal{A},$$

which is Galois by 5.14.

We have checked all cases so the induction is complete. Note that working over fields with Frobenii is only crucial in steps 5 and 6.

Conversely, suppose we have a Galois stratification $\mathcal{A} = \langle \mathbb{A}_{(S, \sigma)}^n, Z_i/X_i, C_i \rangle$. By refining it further, we may assume that each Galois covering $(Z_i, \Sigma_i) \rightarrow (X_i, \sigma)$ with group $(G, \tilde{\Sigma})$ is embedded in some affine space, in the sense that Z_i is embedded in some \mathbb{A}_S^m , and all automorphisms corresponding to elements of G are restrictions of difference rational endomorphisms of \mathbb{A}_S^m to Z_i , and the canonical projection $Z_i \rightarrow X_i$ is a restriction of difference rational morphism $\mathbb{A}_S^m \rightarrow \mathbb{A}_S^n$. Then, if C_i is the conjugacy class of some element $\sigma_i \in \Sigma$, the set

$$\{x \in X_i : \text{ar}(x) \subseteq C_i\} = \{x \in X_i : \exists z \in Z_i^{\sigma_i}, z \mapsto x\}$$

is clearly expressible in a first-order way using an existential formula in the language of difference rings. When C_i is a union of conjugacy classes, we take the disjunction of the corresponding difference ring formulae. \square

Let T_∞ be the set of first-order sentences true in difference fields (\bar{k}, φ_k) with k a sufficiently large finite field.

Corollary 5.17. *The theory T_∞ is decidable by a \dagger -primitive recursive procedure. Moreover, for each first-order sentence $\theta \in T_\infty$ a \dagger -primitive recursive procedure can compute the (finite) list of exceptional finite fields k such that θ does not hold in (\bar{k}, φ_k) .*

Proof. The quantifier elimination procedure produces a Galois stratification \mathcal{A} on the base $S = \text{Spec}(\mathbb{Z})$ and a constant m such that for every $p \in S$, and every k of characteristic p with $|k| \geq m$, $\theta(\bar{k}, \varphi_k) = \mathcal{A}(\bar{k}, \varphi_k)$. The stratification \mathcal{A} stipulates the existence of a localisation $S' = \mathbb{Z}[1/N]$ of S , a Galois cover Z/S' and a conjugacy class C in $\text{Gal}(Z/S')$ such that, for $p \in S'$ (i.e., for p not dividing N), and k of characteristic p with $|k| \geq m$, θ holds in (\bar{k}, φ_k) if and only if $\varphi_k \in C$. By (the classical) Chebotarev's density theorem, this can hold for all but finitely many p if and only if $C = \text{Gal}(Z/S')$, which can be effectively checked by (\dagger_7) .

For each field (\bar{k}, φ_k) with characteristic of k dividing N , or $|k| < m$, once we interpret σ as the Frobenius φ_k with $\varphi_k(\alpha) = \alpha^{|k|}$, the formula θ can be treated as a formula in the language of rings, which can be decided by the well-known primitive recursive decision procedure for the algebraically closed field \bar{k} . \square

A more model-theoretic restatement of the above theorem would say that the theory T_∞ of fields with Frobenii allows quantifier elimination down to the class of Galois formulae. Given that T_∞ happens to be ([13]) the theory of existentially closed difference fields (ACFA), let us state an appropriate analogue of the above result.

We must emphasise that the statement below can be obtained unconditionally, i.e., without appealing to [13], by replacing the use of [19, 5.2] in the present paper by the use of existential-closedness of models of ACFA (i.e., by the use of the 'ACFA-axiom'). This will be done in a separate paper [18].

Theorem 5.18. *Let (k, σ) be a difference field. Let $\psi(x) = \psi(x; s)$ be a first order formula in the language of difference rings in variables $x = x_1, \dots, x_n$ with parameters s from k . There exists a Galois stratification \mathcal{A} of the difference affine n -space over k such that for every model (F, φ) of ACFA which extends (k, σ) ,*

$$\psi(F, \varphi) = \mathcal{A}(F, \varphi).$$

REFERENCES

- [1] The Stacks Project Authors. *Stacks Project*.
http://math.columbia.edu/algebraic_geometry/stacks-git.
- [2] James Ax. The elementary theory of finite fields. *Ann. of Math. (2)*, 88:239–271, 1968.
- [3] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.
- [4] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.
- [5] Jan Denef and François Loeser. Definable sets, motives and p -adic integrals. *J. Amer. Math. Soc.*, 14(2):429–469 (electronic), 2001.
- [6] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.
- [7] M. Fried and G. Sacerdote. Solving Diophantine problems over all residue class fields of a number field and all finite fields. *Ann. of Math. (2)*, 104(2):203–233, 1976.
- [8] Michael D. Fried. Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the Finite Simple Group Classification. [arXiv:1012.5297v5](https://arxiv.org/abs/1012.5297v5).
- [9] Michael D. Fried, Dan Haran, and Moshe Jarden. Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, 85(1-3):103–133, 1994.
- [10] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1986.
- [11] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. *Inst. Hautes Études Sci. Publ. Math.*, (24), 1965.
- [12] Alexandre Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris), 3. Société Mathématique de France, Paris, 2003. Séminaire de

- géométrie algébrique du Bois Marie 1960–61. Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; (50 #7129)].
- [13] Ehud Hrushovski. The elementary theory of the Frobenius automorphism. Preprint, 2004.
 - [14] Catarina Kiefe. Sets definable over finite fields: their zeta-functions. *Trans. Amer. Math. Soc.*, 223:45–59, 1976.
 - [15] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
 - [16] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
 - [17] Johannes Nicaise. Relative motives and the theory of pseudo-finite fields. *Int. Math. Res. Pap. IMRP*, (1):Art. ID rpm001, 70, 2007.
 - [18] Ivan Tomašić. Galois stratification and ACFA.
<http://www.maths.qmul.ac.uk/~ivan/tgsacfa.pdf>, 2012. Submitted.
 - [19] Ivan Tomašić. A twisted theorem of Chebotarev. [arXiv:1210.3571v1](#).
 - [20] Michael Wibmer. A Chevalley theorem for difference equations. [arXiv:1010.5066v1](#).

IVAN TOMAŠIĆ, SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY UNIVERSITY OF LONDON,
 LONDON, E1 4NS, UNITED KINGDOM
E-mail address: i.tomasic@qmul.ac.uk